NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DA VINCI'S CHILDREN TAKE FLIGHT:
UNMANNED AIRCRAFT SYSTEMS IN THE HOMELAND

by

Jeanie Moore

March 2014

Thesis Advisor:	John Rollins
Second Reader:	Robert Simeral

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
DA VINCI'S CHILDREN TAKE FLIGHT: UNMANNED AIRCRAFT SYSTEMS IN THE HOMELAND

5. FUNDING NUMBERS

6. AUTHOR(S) Jeanie Moore

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

In 2015, the Federal Aviation Administration will open national airspace to unmanned aircraft systems (UAS). Nonmilitary uses for UAS range from agriculture services to entertainment purposes, and include tasks as mundane as inspecting gutters and as consequential as fighting fires.

Outside of the safety issues that accompany many breakthrough technologies, the effort to integrate UAS into national airspace is enmeshed in political, legal and economic policies that require careful navigation. Factors like cybersecurity and technological advancements will continue to influence the way UAS can be used.

This thesis provides an orientation to the key considerations in UAS integration. Policy recommendations include early stakeholder engagement; a national data protection law; no-fly zones around private residences; clearly identifying UAS operators and owners; nonlethal payloads in national airspace; adapting current surveillance laws to UAS; a single, national privacy law to facilitate the free flow of commerce and coordination across state lines; a federal office in charge of monitoring data privacy; accountability of data collectors; limited exemptions for activities conducted in the interest of national security or to protect life and property; and managing cybersecurity risks.

14. SUBJECT TERMS Unmanned aerial system; UAV; unmanned aerial vehicle; unmanned aircraft systems; technology; change; stakeholder engagement; policy; future; privacy; human rights; civil liberties; civil liberty; innovation

15. NUMBER OF PAGES
115

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DA VINCI'S CHILDREN TAKE FLIGHT: UNMANNED AIRCRAFT SYSTEMS IN THE HOMELAND

Jeanie Moore
Acting Director, Private Sector Division, Office of External Affairs,
Federal Emergency Management Agency
B.A., College of Charleston, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
March 2014

Author: Jeanie Moore

Approved by: John Rollins, Contractor
Thesis Advisor

Robert Simeral
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In 2015, the Federal Aviation Administration will open national airspace to unmanned aircraft systems (UAS). Nonmilitary uses for UAS range from agriculture services to entertainment purposes, and include tasks as mundane as inspecting gutters and as consequential as fighting fires.

Outside of the safety issues that accompany many breakthrough technologies, the effort to integrate UAS into national airspace is enmeshed in political, legal and economic policies that require careful navigation. Factors like cybersecurity and technological advancements will continue to influence the way UAS can be used.

This thesis provides an orientation to the key considerations in UAS integration. Policy recommendations include early stakeholder engagement; a national data protection law; no-fly zones around private residences; clearly identifying UAS operators and owners; nonlethal payloads in national airspace; adapting current surveillance laws to UAS; a single, national privacy law to facilitate the free flow of commerce and coordination across state lines; a federal office in charge of monitoring data privacy; accountability of data collectors; limited exemptions for activities conducted in the interest of national security or to protect life and property; and managing cybersecurity risks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. PROBLEM SPACE....2
- B. RESEARCH QUESTIONS....6
- C. METHOD....7
- D. LITERATURE REVIEW....9
- E. OVERVIEW OF CHAPTERS....25

II. RADICAL CHANGE, RISK AVERSION AND THE TRIUMPH OF PUBLIC OPINION....27
- A. PROSPECT THEORY (RISK AVERSION)....29

III. STAKEHOLDER ENGAGEMENT....31
- A. STAKEHOLDER GROUPS....32
- B. SUMMARY....36

IV. CONVERGING PATHS: CYBERSECURITY, UNMANNED SYSTEMS AND THE RISE OF TRANSPARENCY....39
- A. PUBLIC AND PRIVATE SECTOR ROLES IN SOLVING CYBERSECURITY THREATS....43

V. THE LEGAL AND CONCEPTUAL CHALLENGES OF PRIVACY....47
- A. THE EU AND UK APPROACH....51
- B. TOWARD A POLICY OPTION TO PROTECT PRIVACY WHILE MAINTAINING TRANSPARENCY....53
- C. ADVOCACY ORGANIZATIONS....56
- D. RECOMMENDATIONS FOR APPLYING EU AND UK GOOD PRACTICES IN THE U.S.....56

VI. FUTURE CONSIDERATIONS, ANALYSIS AND RECOMMENDATIONS....59
- A. FUTURE SCENARIOS 2050....59

VII. ANALYSIS....63
- A. COSTS....64
- B. COURSES OF ACTION....64
- C. POLICY RECOMMENDATIONS....67
- D. MEASURING SUCCESS....70
- E. CONCLUSION....71
- F. RECOMMENDATIONS FOR FUTURE RESEARCH....72

APPENDIX A. USEFUL LINKS....75

APPENDIX B. COMPARISON OF KEY PRIVACY RULES IN U.S., EU....77

LIST OF REFERENCES....83

INITIAL DISTRIBUTION LIST....89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Map of Countries that Acquired UAS by December 2011. 4
Figure 2. Examples of Current Uses for UAS and their Altitudes of Operation.....13
Figure 3. Sample of Unmanned Systems https://ieeexplore.ieee.org/ieee_pilot/articles/96jproc12/jproc-RWeibel-2006118/article.html 14
Figure 4. NonFederal Recipients of Certificates of Waiver or Authorization and Special Airworthiness Certificates in the Experimental Category and the Location, as of July 13, 2012. 15
Figure 5. Selected UAS Test Site Operators 16
Figure 6. Conceptual Map of Stakeholders with an Interest in UAS in American National Airspace and Influencing Factors.....31
Figure 7. Map of Congressional Representation on Senate and House UAS Caucuses, Overlaid with the Six FAA-Approved UAS Test Sites as of December 31, 2013. 32
Figure 8. Change Dynamics Process Model. 37
Figure 9. Cybersecurity Issues During UAS Production 41
Figure 10. Timeline of Privacy in America.....49

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ALPA	Air Line Pilots Association
ACLU	American Civil Liberties Union
ANSI	American National Standards Institute
AUVSI	Association for Unmanned Vehicle Systems International
CoA	certificate of authorization
CEO	chief executive officer
CCTV	closed circuit television
CRS	Congressional Research Service
CBP	Customs and Border Protection
DHS	Department of Homeland Security
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
EU	European Union
FAA	Federal Aviation Administration
GPS	Geospatial Positioning System
GAO	Government Accountability Office
IEEE	Institute of Electrical and Electronics Engineers
IRS	Internal Revenue Service
IACP	International Association of Chiefs of Police
NASA	National Aeronautics and Space Administration
NSA	National Security Agency
SLTT	state, local, tribal, territorial
TSA	Transportation Security Administration
U.K.	United Kingdom
UAS	Unmanned Aircraft Systems

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

A. INTRODUCTION

In 2015, the Federal Aviation Administration (FAA) will introduce rules that open up national airspace to unmanned aircraft systems (UAS), also commonly called drones. Until 2012, when Congress included a mandate for this action in the FAA appropriations, UAS were primarily used by the military for training and for overseas support. The National Aeronautical and Space Administration (NASA) has also been developing high-altitude UAS. More recently, small UAS have been available to hobbyists, but they are not allowed to occupy the same airspace as manned aircraft.

This looming deadline is a focal point for entrepreneurs and lobbyists, civil liberties advocates and lawmakers, as well as others who are following this topic. Unmanned vehicles offer enormous design flexibility since they are not constrained in size or structure by a requirement to carry a human operator. In addition to virtually unlimited airframe options, the sensor technology that UAS can carry is exceptionally advanced. These two factors alone open the way for a multitude of new, nonmilitary uses for UAS in areas that range from agriculture to emergency services to entertainment, to tasks as mundane as inspecting gutters or any other activity that might benefit from an aerial approach.

Outside of the safety issues that accompany many breakthrough technologies, the effort to integrate UAS into national airspace is enmeshed in politics, legal issues, economics, and other issues that require careful navigation. There are also influencing factors like cybersecurity and technological advancements like autonomy, which will change the way UAS can be used.

B. RESEARCH QUESTIONS

This thesis explores a range of vastly different, but interrelated issues that may impact the success of UAS integration, within the context of homeland security. A central question is “How might domestic civilian and government UAS use shape the homeland security environment?” Supporting questions that guide this research include:

- What are the potential uses for UAS in the homeland security context? What are the potential threats?
- What types of UAS technology are available—and to whom? What is the current range of UAS capabilities?
- How is the UAS issue being framed in public discussion? What is the potential impact of media and public opinion on UAS use for homeland security purposes?
- Who are the influential stakeholders? What aspects of the debate do they influence? How are they connected?
- What technologies and laws define privacy today? How do Americans understand privacy in the 21st century?
- Are UAS a disruptive technology when used in the domestic airspace?

C. METHOD

The research methods included a qualitative analysis of the growing body of literature on UAS, as well as a policy options analysis. A range of literature was reviewed, including reports from the Government Accountability Office and the Congressional Research Service, congressional testimony, government websites and publications, industry and private sector research, civil liberties groups, domestic and foreign laws, media coverage and consultation with subject matter experts. Action research offered insight into the stakeholder environment.

The final result is intended to be orientation to key issues and considerations in UAS integration for the nontechnical homeland security practitioner and other stakeholders.

D. FINDINGS

Although UAS have been in use since the early to mid-20th century, they may be a disruptive innovation as they enter the commercial market. In his book *The Innovator's Dilemma*,[1] Clayton Christensen describes a disruptive technology as one that may start as a niche market for just a few consumers—perhaps even something with less utility than the original version—but nevertheless a technology that rapidly overtakes the sustaining

[1] Clayton Christensen, *The Innovator's Dilemma* (New York: HarperBusiness, 2000).

technology of the day. Examples include the switch from main frame to desk top computing, land lines to cell phones, and horses to automobiles.

In the face of change on the scale of the pending introduction of UAS in national airspace—especially with so many unknowns— it is natural for people to resist change. In his book *Thinking Fast and Slow*, Nobel Prize-winning economist Daniel Kahneman explains this risk aversion through prospect theory.[2]

"The brains of humans and other animals contain a mechanism that is designed to give priority to bad news," Kahneman says. "Loss aversion is a powerful conservative force that favors minimal changes from the status quo in the lives of both institutions and individuals. This conservatism helps keep us stable in our neighborhood, our marriage, and our job; it is the gravitational force that holds our life together near the reference point."[3]

Another theory that may help explain how the American population might react to the relatively sudden introduction of UAS is Georgetown professor Fathali Moghaddam's Micro-Macro Rule of Change.[4] Moghaddam, an author and expert in psychology and terrorism, explains that rapid changes at a macro, or societal level, may trigger a psychological disconnect at the micro, or individual, level.[5] Coupled with prospect theory, the Macro-Micro rule of change might forecast a strong sense of angst and possibly social unrest as the American population acclimates to the relatively sudden introduction of UAS in 2015.

E. KEY ISSUES

While the FAA focuses on safety, there are several other issues that will influence the environment within which UAS integration is taking shape. These issues include rapid advances in technology, such as autonomous robotics (requiring no human

---

[2] Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux): 283–286, 305.

[3] Ibid.

[4] Fathali M. Moghaddam, *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy* (Westport, CT: Praeger, 2006), 130.

[5] Ibid.

guidance), increasingly precise sensor technology that can consume vast amounts of data, the lack of consistent laws to protect privacy, and rapidly growing cybersecurity vulnerabilities.

F. STAKEHOLDER ENGAGEMENT

The complex stakeholder environment creates its own set of tensions. A diverse mix of industry lobbyists, civil liberties advocates, researchers and students, media, emergency responders and congressional interests all carry their own agendas into the discussion. Figure 1 provides a high-level illustration of these interrelationships.

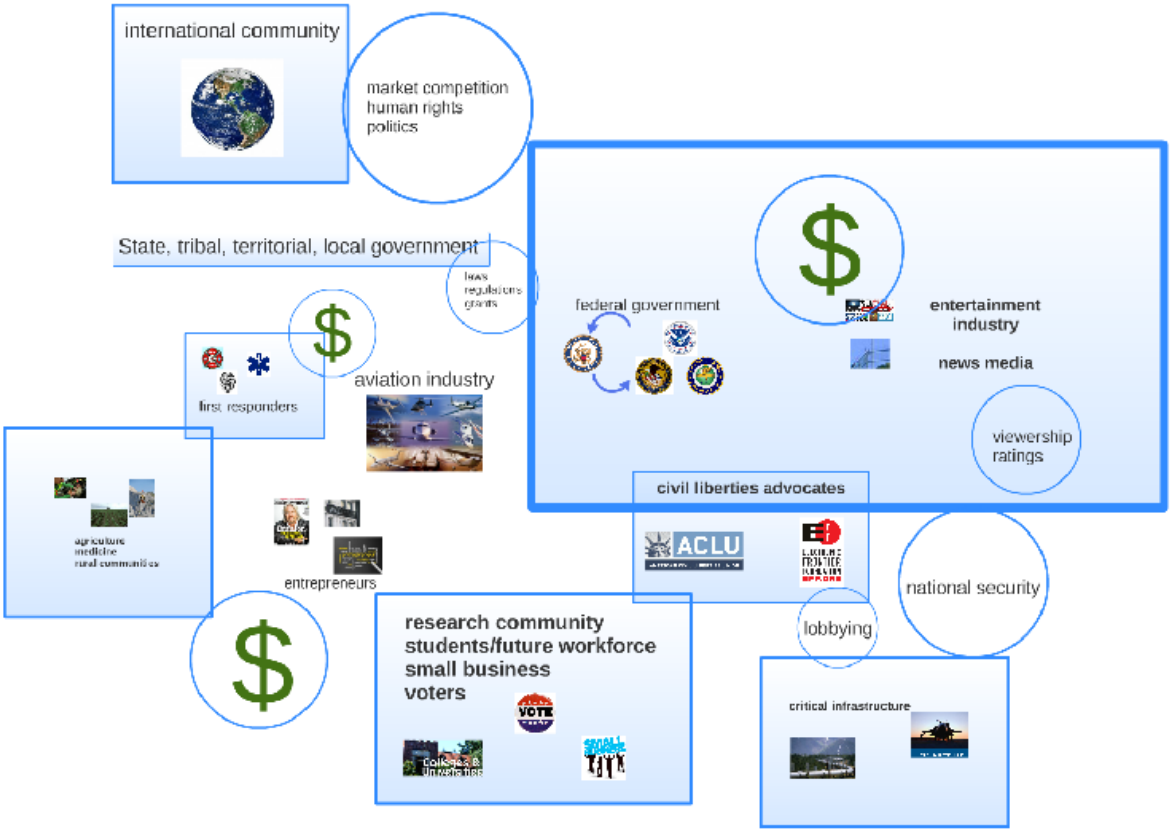


Figure 1. Conceptual Map of Stakeholders with an Interest in UAS in American National Airspace and Influencing Factors.

G. CYBERSECURITY

In an era of increasing transparency and increasing access to massive amounts of data, concerns over persistent surveillance and privacy create another layer within the UAS integration debate. Compounding these is a growing understanding of just how vulnerable technology across the board is to cyber-attacks.

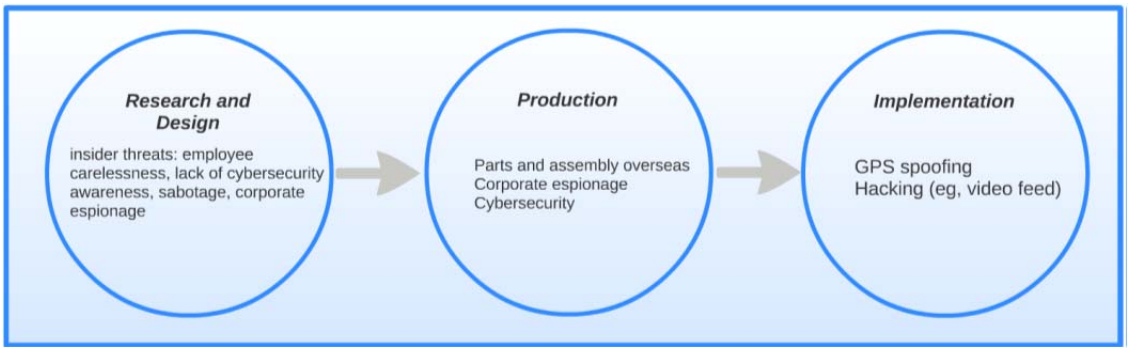


Figure 2. Cybersecurity Vulnerabilities during UAS Production

H. LEGAL ISSUES

The concept of privacy is exceptionally subjective. Americans in particular are notoriously protective of their privacy, while at the same time highly reliant on mobile phones, GPS, Internet communications, credit cards and other technology that tracks our every move. At present, the laws governing privacy are an amalgam of federal, state and local laws that have been created to address specific issues- often as new technology is introduced, as shown in Figure 3. However, there is no single, nationally applicable privacy law—not even the commonly referenced 4th Amendment covers the issues that arise in the UAS debate. In contrast, the European Union—and in particular the United Kingdom where CCTV is commonly used for law enforcement—have developed consistent laws that balance security needs with individual privacy.

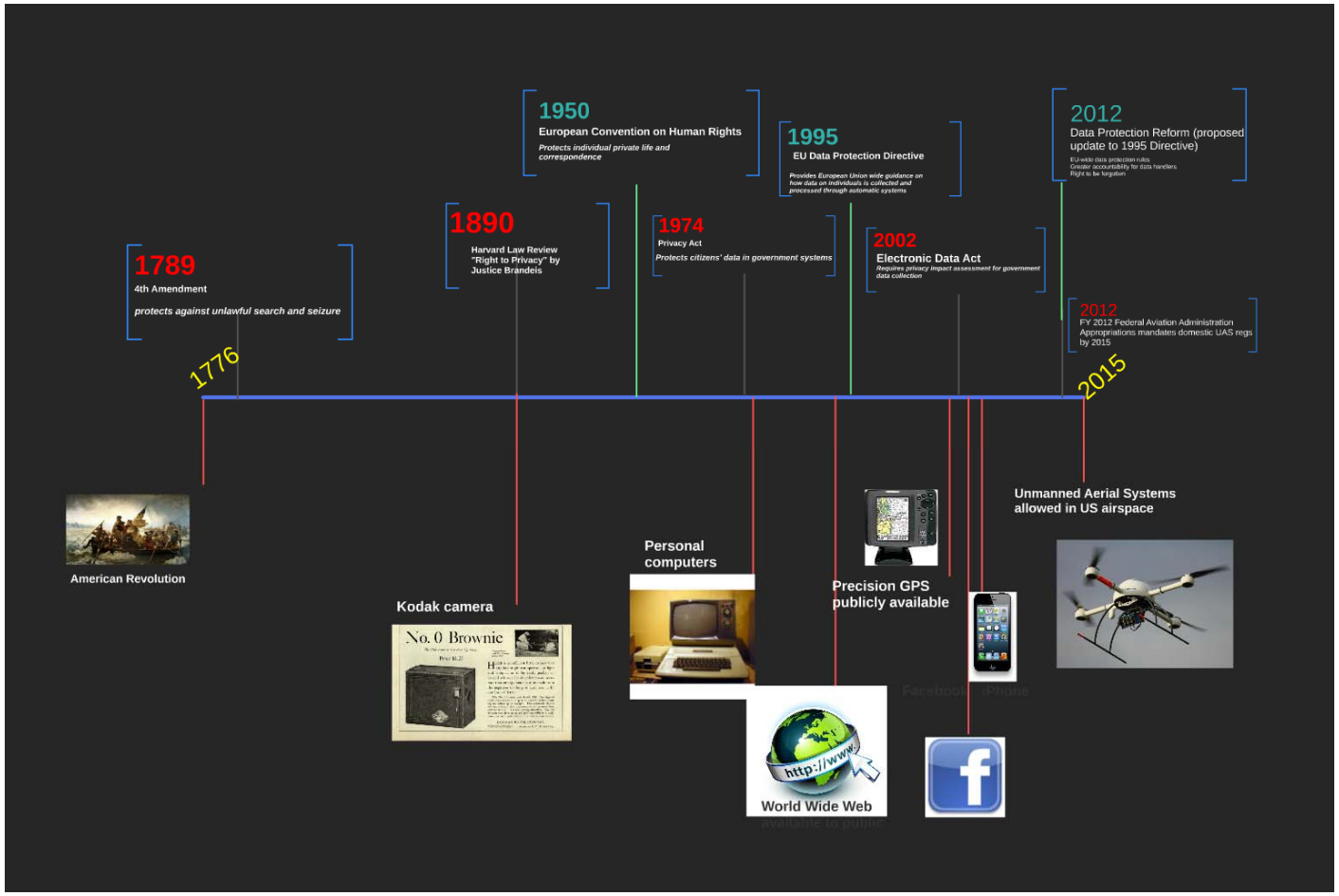


Figure 3. Timeline of Privacy in America[6]

[6] Photos, Prezi.com, accessed January 12, 2014. https://prezi.com/.

Landmark legislation includes Article 8 of the European Convention on Human Rights, EU Directive 95, and the Safe Harbor Initiative. More recently, the 2012 Data Protection Reform Act was introduced to update EU Directive 95. Notable points in this initiative include:

- A single set of data protection rules valid across the EU
- Increased responsibility and accountability for those processing personal data
- A "right to be forgotten" to help people better manage data-protection risks online

I. ANALYSIS

While the issues vary greatly, all of the topics discussed in this thesis are connected and should be addressed comprehensively. In the context of UAS integration, cybersecurity impacts privacy, safety and economic interests. Legal issues touch all of these areas, and yet laws struggle to keep pace with technology.

Given the broad range of stakeholder agendas related to UAS integration, it will be important to engage media, advocacy groups, Congress, industry, academia, emergency responders and all of the other stakeholders in a transparent policy development process.

J. POLICY RECOMMENDATIONS

Building on the work already conducted by a variety of interest groups on both sides of the issue, this thesis offers 10 policy recommendations:

- Establish boundaries, including no-fly zones around private residences, to protect privacy
- Encourage accountability by clearly identifying UAS operators and owners, such as through a UAS version of the Department of Motor Vehicles
- Engage stakeholders early and often at all levels; let the market drive demand, especially for emergency and homeland security activities
- Employ only nonlethal payloads in national airspace
- Adapt current surveillance laws to UAS

- Develop a single, national privacy standard to facilitate the free flow of commerce and coordination across state lines
- Establish a federal office in charge of monitoring data privacy, with state-based field offices to streamline oversight of data collection, aggregation and disposal
- Enforce accountability of data collectors, holding them responsible for the protection and disposal of personally identifiable information
- Provide limited exemptions for activities conducted in the interest of national security, life safety, and protection of property, such as surveying pre- and post-disaster damage
- Manage risk and enforce cybersecurity at all levels, in partnership with the private and public sectors

K. CONCLUSION AND RECOMMENDATIONS

The deadline to integrate UAS into national airspace is almost here. Will this initiative be successful? Will government or the private sector drive UAS integration forward—or both? Efforts to put thoughtful policies in place today will have economic, security, and privacy impacts that reach well into the future. Poorly developed policy- or no policy at all- could steer the future toward an era of increased surveillance and diminishing security. An attempt to back out of the global UAS market could leave the U.S. at a severe economic disadvantage in a growing, multi-billion dollar industry. In the best case, excellent policies will be developed in close collaboration with the many stakeholder groups, resulting in new job opportunities, better and cheaper airborne services, increased safety and security and a system that is well adapted to serve human needs, rather than one that imposes itself on the population.

Future research opportunities abound, as this area develops. Some areas for consideration include emerging technology like autonomy and 3-D printing, and how these technologies will impact UAS safety and accountability; cybersecurity issues and UAS integration; or additional public opinion surveys.

Just as engineer/inventor/artist Leonardo Da Vinci faced seemingly insurmountable challenges on the political and social fronts, current proponents of UAS integration must work against a natural predisposition to the status quo to gather widespread support for a technology that will bring about rapid, macro-level change.

Whether one believes that today's population is better prepared to adapt, having been primed by a world that is already technologically advanced, or that technology is advancing too fast to keep up, the policies we put in place and decisions taken today will have impacts far into the future. There is still time to get it right, but the window is closing fast.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

No undertaking as daunting as completing a rigorous master's degree while holding a full-time job can be accomplished solo. This thesis was possible only with the help of the following:

- My brilliant husband, who persuaded me to take this journey and shared many a conversation over 4 a.m. coffee; who has borne more than his fair share of the responsibility for our home; and who has single-handedly kept our lives on track for the past 18 months, yet never stopped encouraging me along the way.
- My professors at the Center for Homeland Security and Defense, who re-awakened my long-dormant curiosity and reinvigorated my intellect, and who persistently gave of themselves and their vast experience.
- My thesis advisor John Rollins and reader Robert Simeral, who gave me free reign to experiment and gently nudged me back on track when I followed too many interesting rabbit trails.
- My cohort, who never stopped challenging me and who have collectively made me a better person. I will miss our discussions more than you know.
- My parents, who gave me a love of flight, who taught me to read the clouds and to love the smell of small airports.

My deepest gratitude to you all.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> *Once you have tasted flight, you will forever walk the earth with your eyes turned skyward, for there you have been, and there you will always long to return.*
>
> —Artist, engineer and innovator Leonardo da Vinci

The U.S. is on the brink of a new era in aviation, one that has the potential to impact nearly every aspect of how Americans move goods, protect critical infrastructure, respond to emergencies, and monitor environmental issues. In 2015, the Federal Aviation Administration is scheduled to release guidelines that open up domestic airspace to widespread use of unmanned aircraft systems (UAS), a technology that is virtually unlimited in its potential uses since the size and structure does not need to accommodate a human pilot. With the advent of widespread UAS use in a nonmilitary capacity, a new industry will emerge, requiring new laws, new technology and new training.[1]

Significant change over a short period of time can create societal breakthroughs or, if implemented thoughtlessly, the potential benefits could be buried under public backlash or even lead to undesired consequences. Given the significance of opening up national airspace to UAS for government and commercial purpose, it is important that policy makers come together with stakeholders to create a clear vision and a strategic path to the desired end state.

The environment within which these developments are unfolding is dynamic, exciting and filled with potential. Machines are getting smarter, faster and more connected. Economic opportunities are beckoning, and the wheels of innovation are spinning up new ways to improve our lives. But there are also perils: cybersecurity, loss of privacy and safety among them.

---

[1] Teal Group, "Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast," news release, April 11, 2012. http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/66-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast. Aerospace industry analyst Teal Group released a 2012 study forecasting annual expenditures to double over the next 10 years, for a total of $89 billion in global expenditures—nearly double the current rate of expenditures—with the U.S. leading research and development at 62% of the market, and accounting for 55% of acquisitions.

At the time this thesis was being researched, Edward Snowden's leaks about National Security Agency surveillance exploded in the news, as did coverage of U.S. military drone strikes overseas. These issues cannot help but color the discussion of introducing UAS at home.

A. PROBLEM SPACE

The introduction of UAS in the domestic airspace is a complex and polarizing issue. This thesis will attempt to unravel some of the key questions lingering in the minds of stakeholders ranging from advocates to lawmakers, and develop a realistic picture of the environment and possible paths forward.

Looking at the just the nontechnical aspects, there are at least six critical issues at play:

- **Privacy:** The U.S. population is uniquely protective of its privacy compared to other democratic nations like the U.K., which regularly uses CCTV for surveillance in public spaces. Implicit protections for individual privacy are embedded in the U.S. Constitution through the 4th Amendment.
- **Legal Structure**: There is no single, overarching privacy law that can be applied nationwide; instead there is a hodge-podge of federal, state and local laws that can vary significantly
- **Accelerating Technology:** Technology is advancing far faster than a bureaucracy can pass sensible laws to manage the new technology.
- **Economics:** As other countries start to adopt UAS domestically for various purposes, the U.S. may be left at a competitive disadvantage in a growing industry worth potentially tens of billions of dollars- or more.
- **Public Perception**: The media is casting an increasingly critical eye on U.S. military targeted strikes overseas, and Congress has held special hearings on the issue. Key concerns bubbling up include the lack of public discussion on the use of UAS, dehumanizing war and general ethics of remote killing. Domestically, many opponents equate UAS with military drones, making it difficult to separate the issues for domestic and commercial use.
- **Cybersecurity:** Concurrent with, but not directly related to, the rise of UAS is a growing awareness of the inherent vulnerabilities in technology that relies on the Internet although not a widespread issue at present, it is possible for UAS sensors and guidance systems to be hacked. In fact, in 2012, Iran hijacked a U.S. RQ-170 drone, claiming to have used GPS

> spoofing to safely land and secure it. If foreign press can be believed, there are concerns in Pakistan that terrorist organizations are attempting to gain the technical expertise to conduct similar attacks on drones used to patrol Pakistani borders.[2]

As a disruptive technology, domestic UAS are igniting public debate over important issues like civil liberties and safety. They are also inspiring new markets and innovative approaches to old problems, such as how to tackle "dull, dirty and dangerous" jobs like monitoring thousands of miles of natural gas pipelines or large agriculture enterprises.

While the FAA is working on how best to integrate UAS safely into an already crowded airspace, federal policies may not be able to keep pace with the civil liberty issues that may arise with a boom in the use of UAS and the highly advanced sensors that they can carry. So how do we balance legitimate homeland security needs with market pressures and the interests of an open society?

At present, UAS may be operated legally on an extremely limited basis, and only if a Certificate of Authorization (CoA) can be obtained from the FAA. In January 2014, the Federal Aviation Administration (FAA) awarded CoAs to the first six test sites nationwide. While small UAS are available commercially, they are commonly limited to low-flying toys for hobbyists, such as quadcopters.

1. Developing Supporting Policy

Foreseeing a world in which UAS are as commonplace as refrigerators, a number of organizations have started to draft proposed guidance to address civil liberties and privacy issues. These organizations range from the International Association of Chiefs of Police (IACP), to the ACLU and Privacy Now, to state and local lawmakers. However, there is not yet a single, nationwide policy in place.

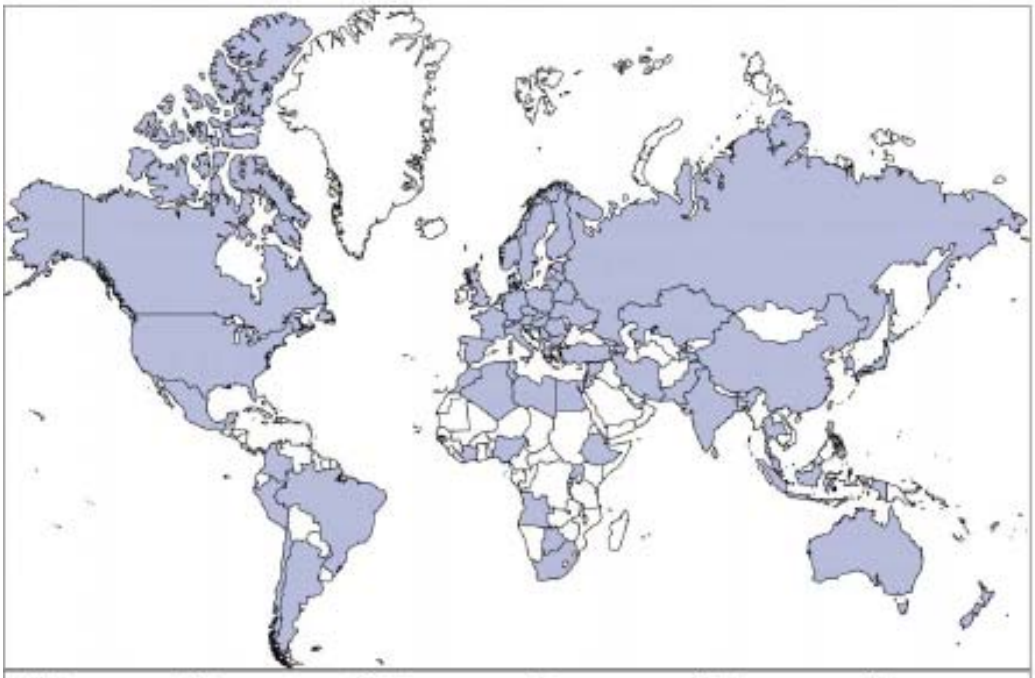
Successful integration of UAS into domestic airspace will require attention to safety and civil liberties. It will also need to take into account economic drivers, emerging cybersecurity issues, the advancement of autonomy, and public opinion.

---

[2] Yatish Yadav, "UAVs Prone to Hacking, Warn Intel Agencies," *Indian Express*, July 25, 2013. http://www.newindianexpress.com/nation/UAVs-prone-to-hacking-warn-intel-agencies/2013/07/25/article1700651.ece#.UwkD0mJdXhc.

2. Growing Market Competition

Delaying the 2015 congressional deadline could put the U.S at a significant competitive disadvantage in a booming global UAS technology market. Currently, over 70 allied nations and a number of nonallied nations are actively exploring or even using UAS at home.[3] Figure 1 shows the countries that acquired UAS technology as of 2011.



Algeria	Chile	Greece	Libya	Poland	Syria
Angola	China	Hungary	Lithuania	Republic of Korea	Taiwan*
Argentina	Colombia	India	Malaysia	Romania	Thailand
Australia	Croatia	Indonesia	Mexico	Russia	Trinidad and Tobago
Austria	Czech Republic	Iran	Morocco	Serbia	Tunisia
Azerbaijan	Denmark	Israel	Netherlands	Singapore	Turkey
Belarus	Egypt	Italy	New Zealand	Slovakia	Uganda
Belgium	Estonia	Ivory Coast	Nigeria	Slovenia	Ukraine
Botswana	Ethiopia	Japan	Norway	South Africa	United Arab Emirates
Brazil	Finland	Jordan	Pakistan	Spain	United Kingdom
Bulgaria	France	Kazakhstan	Panama	Sri Lanka	United States
Burundi	Georgia	Latvia	Peru	Sweden	
Canada	Germany	Lebanon	Philippines	Switzerland	

Sources: GAO analysis of various unclassified sources; Map Resources (maps).

Note: Shaded countries have acquired UAV systems.

Figure 1. Map of Countries that Acquired UAS by December 2011.[4]

---

[3] U.S. Air Force. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047*. (Washington, DC: USAF Headquarters, May 18, 2009); Teal Group, "Group Predicts."

[4] Thomas Melito, *Nonproliferation: Agencies Could Improve Information Sharing and End Use Monitoring on Unmanned Aerial Vehicle Exports*. GAO -12-536 (Washington, DC: GAO Government Accountability Office, 2012), 10.

3. A Matter of Public Opinion

At least one recent public opinion survey found that the general population would accept commercial and humanitarian use of UAS,[5] although a growing number of states and local municipalities such as Charlottesville, VA, and Seattle, WA, have taken pre-emptive steps to prevent law enforcement use of UAS.[6]

However, bad press could work against the UAS industry, slowing down integration or even killing the effort altogether if there is enough pushback from the public, as in the case of the now-defunct DHS Office of Intelligence and Analysis National Applications Office. The concept behind this program was sound enough, in that it was an attempt to create a cost-saving approach to developing a Department-wide capability for gathering detailed imagery through satellites and other platforms. This imagery could have been used in legitimate homeland security missions, such as disaster support. However, lacking a strong public outreach component, the program could not get past public misconceptions and fears that this effort would lead to illegal surveillance on American citizens and invasion of privacy. Instead, individual components have had to explore various options on their own, without the economies (and savings to tax payers) that an integrated, Department-wide initiative could have brought.

Countering the potential drag of negative public opinion, commercial interests are pushing UAS integration forward as the consumer demand rises. There is a rapidly growing underground market as companies from across the spectrum of the private sector are picking up on tremendous opportunities that UAS can offer.[7]

The general public is already becoming accustomed to low-altitude "toy" UAS such as Verizon's "Parrot" quadcopter that can be controlled through a mobile device, and small UAS are featured in a 2014 Lexus commercial, drawing an association with

---

[5] Joe Eyerman et al., *Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns* (Research Triangle Park, NC: Institute for Homeland Security Solutions, 2013), 2–6.

[6] Somini Sengupta. "Rise of Drones in U.S. Drives Efforts to Limit Police Use," *New York Times*, February 15, 2013.

[7] Chris Francescani, "From Hollywood to Kansas, Drones Are Flying under the Radar," *Reuters*, March 3, 2013. http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303.

high tech luxury. Driven by commercial and private use, it is a relatively small step for public acceptance of much broader market uses, including homeland security and law enforcement use. Allowing the market to drive demand may ultimately benefit law enforcement and emergency services, if the public creates the demand for UAS rather than having UAS forced on them.[8]

B. RESEARCH QUESTIONS

A new world is emerging, one in which unmanned systems will take their place alongside human operators in the sky, on land and in the sea. Unmanned aircraft systems (UAS) in particular are on the verge of crossing over into the mainstream.

Since 2012, the FAA has been preparing to enact regulations that allow UAS to be used domestically by 2015.

This thesis will examine domestic UAS use as a disruptive technology with far-reaching homeland security impacts. In particular how might domestic civilian and government UAS use shape the homeland security environment?

Supporting questions include:

- What are the potential uses for UAS in the homeland security context? What are the potential threats?
- What types of UAS technology are available- and to whom? What is the current range of UAS capabilities?
- How is the UAS issue being framed in public discussion? What is the potential impact of media and public opinion on UAS use for homeland security purposes?
- Who are the influential stakeholders? What aspects of the debate do they influence? How are they connected?

[8] There is also a role for standards organizations like the ANSI Homeland Security Standards Panel to develop consistent guidelines that will support interoperability of various UAS communications systems, as well as the adoption of UAS in a safe and publicly acceptable manner. Developing interoperable communications will increase safety efforts by enabling manned flights to communicate with UAS operators. It would also significantly increase joint law enforcement and homeland security efforts, allowing greater real-time information sharing, as encouraged in numerous strategies, including Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.

- What technologies and laws define privacy today? How do Americans understand privacy in the 21st century?
- Are UAS a disruptive technology when used in the domestic airspace?

C. METHOD

1. Qualitative Analysis

A qualitative analysis of current literature will help identify and explore nontechnical issues associated with UAS integration into national airspace, with the homeland security practitioner in mind. Due to the extensive impact of the issue across a wide variety of stakeholders, action research will supplement the literature review as a way to develop a stakeholder engagement angle of a policy options analysis, suggesting paths that the U.S. might take to ensure a balanced approach to meeting homeland security and market demands as UAS are integrated in to national airspace.

Since UAS are still very new in national airspace, further research will include a review of related literature on recent and emerging technologies that have also raised civil liberties, such as CCTV use in the European Union and the United Kingdom. These regions have democratic values similar to those of the U.S., allowing relevant comparisons to be drawn between their approaches to privacy issues when using CCTV.

2. Policy Options Analysis

Policy options will be developed based on promising practices identified in the literature review, as well as by aggregating and synthesizing proposed rules offered by advocacy groups and legislators. Proposed criteria for measuring policy outcomes could include:

- **Policy keeps pace with market demands.** The United States enjoys a free market economy that is protected by laws, even within the arena of homeland security. If policies are not developed with this in mind, then the market will find alternate routes to meet consumer demand.
- **Public interest is considered, as expressed through political leadership.** Public interest will be assumed to coincide with political acceptability, since lawmakers are expected to be the voice of their voters. A policy that is highly inflammatory to voters (and therefore likely to hurt a political career) is unlikely to succeed.

- **Media coverage is positive or neutral.** The media is a key gatekeeper of information and the ways in which media frame an issue can significantly influence popular opinion. Optimally, media support will help build public support for the policy. At a minimum, neutral media coverage will not hinder policy implementation.
- **Fundamental values are protected.** The balance between Constitutional rights, inherent national values and homeland security should be maintained in the development of new policies. It may be worth establishing a benchmark to define these values and avoid a slippery slope.

Sample: The sample used for this research includes literature produced by the UAS industry, key interest groups on both sides of the issue, Congressional Research Service (CRS) reports, Government Accountability Office (GAO) reports, think tank publications and media coverage. It also includes key privacy laws.

Scope: The wealth of possible domestic use for UAS is incredibly broad, spanning nearly every aspect of government, commercial and private use. For the purpose of this thesis, and in keeping with the emergent nature of this issue, the scope will include a handful of diverse, but connected issues of which homeland security practitioners and decision makers should be aware.

Data Sources: A wide net will be cast to ensure a comprehensive and balanced inquiry into the subject of this thesis. Data sources will include a literature review, subject matter expert consultation, media coverage and legislative milestones to illustrate key aspects of the debate. Further detail is provided below:

Literature Review: The literature review will cover issues related to privacy, the global market for UAS, UAS technology, disruptive technology and the psychological impacts of macro-level change.

- Primary sources: Laws, regulations, congressional testimony, House and Senate bills, Department of Defense long-term strategies, and sample state and local legislation.
- Secondary sources: Congressional Research Service reports, Government Accountability Office reports, industry and advocacy literature, journal articles and videos, websites and think tank publications.

Subject Matter Experts: Experts including government officials from across the Department of Homeland; professional researchers, think tank experts, and possibly private industry experts may be consulted for background research. If available, unstructured conversations may also include representatives of the leading industry and activist groups.

Output: An initial look into the subject yields a complex blend of politics, economic interests, media influence, an evolving definition of privacy, and technological impacts. While the much of the paper offer recommendations on how to address the privacy issue, it is anticipated that the research will also provide a more complete understanding of the environment within which the debate over UAS integration is being conducted.

The final product may be considered an orientation to UAS for the nontechnical homeland security practitioner and other interested parties. Through this analysis, it is hoped that readers ranging from policy makers and journalists to students and interested citizens can better understand the influential factors and key considerations in domestic UAS use as they make their own decisions on efforts in this area.

D. LITERATURE REVIEW

There is a rapidly growing body of literature on the introduction of UAS in the U.S. This work includes Congressional Research Service (CRS) and Government Accountability Office (GAO) reports, congressional hearings, news coverage, theses, and industry and advocacy publications. There is also draft state legislation on UAS use for surveillance, as well as the less formal, but more passionate, online discussion created by readers of mainstream news articles.

Within this literature, there are strong currents of pro-industry advocacy, as an emerging global market worth billions of dollars dangles almost within reach. There is also a thread of unease communicated by those who foresee the potential for civil liberties abuses or even a future where autonomous UAS take their place in the “Internet of Things,” making potentially lethal decisions without human oversight.

1. Who Uses UAS?

Like many widely used technologies such as cell phones, GPS and the Internet, UAS originated with the military. Although the military is still the primary customer, the appetite for adapting UAS capability to domestic use has grown rapidly in both the public and commercial sectors, already outpacing legal considerations. Aerospace companies are anticipating new growth markets and a handful of colleges are already creating degree programs for UAS operators.[9] Law enforcement agencies want to use UAS to monitor and fight crime; homeland security agencies like Customs and Border Protection have already started using UAS on a limited basis to conduct border patrols, search and rescue missions and even support firefighting. There is also vast potential for commercial use, ranging from monitoring gas pipelines and other critical infrastructure, to film-making, agriculture and cargo. In fact, some modern barnstormers like Team BlackSheep have already started using small UAS to film global landmarks, and at least one enterprising REALTOR® uses UAS to film high-end property for marketing purposes.[10] .

2. Military Use

Drones have become increasingly common overseas since the Vietnam War, especially in "dull, dirty and dangerous"[11] situations like extended surveillance or conducting highly targeted missions in enemy territory.[12] Current Department of Defense strategic plans focus on expanding UAS capability across all branches. One development since December 2012 has been the Navy's tests of aircraft carrier catapult launch and

---

[9] Isolde Rafter, "Anticipating Domestic Boom, Colleges Rev up Drone Piloting Programs," *NBCNews.com*. January 29, 2013.

[10] *Rise of the Machines*. Journeyman TV, online documentary, produced by Mark Corcoran and Janet .E Silver, October 15, 2012, http://www.journeyman.tv/?lid=64311.

[11] Bart W. Darnell, "Unmanned Aircraft Systems: A Logical Choice for Homeland Security Support," (master's thesis, Naval Postgraduate School, 2011).

12 Robert G. Moose, "Covering The Homeland: National Guard Unmanned Aircraft Systems Support for Wildland Firefighting and Natural Disaster Events" (Master's thesis, Naval Postgraduate School, 2008). Although the Department of Defense primarily focuses its efforts outside national boundaries, through Defense Support to Civil Authorities, the military (commonly through the National Guard) may provide support within the U.S.—for example, during catastrophic disasters like Hurricane Sandy in 2012. (At least one thesis, "Covering the Homeland: National Guard Unmanned Aircraft Systems Support for Wildland Firefighting and Natural Disaster Events" proposed equipping the National Guard with UAS to support all hazards response.)

arrested recovery of an X-47B UCAS-D[13] — a dangerous maneuver for any aircraft, on a relatively short, moving runway.

In 2007, the Department of Defense issued a 25-year joint Unmanned Systems Roadmap which covers air, ground and maritime systems. The Roadmap notes that positive media coverage of the use of unmanned systems for humanitarian and scientific work will ease privacy concerns and that "[s]ocietal acceptance typically leads to market growth, which stimulates R&D that can lead to more capable, less costly unmanned systems for defense."[14]

In 2009, the U.S. Air Force issued a 50-year implementation strategy. The United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047 cites "persistence, endurance, efficiency and connectivity" as reasons why UAS have become increasingly in demand across the joint forces. Along with increased capability, the Flight Plan envisions a grand scheme to "harness increasingly automated, modular, globally connected, and sustainable multi-mission unmanned systems."[15] There is also is a focus on presenting career paths to "build a foundation for the development of officer and enlisted aircrew with UAS experience."[16]

A year after the release of the Air Force strategy, the Army released its own 25-year plan, the U.S. Army Unmanned Aircraft Systems Roadmap 2010–2035.[17] This document looks at current gaps and future requirements that evolve from protecting ground forces and conducting surveillance to medical evacuations and ferrying cargo.

While these documents offer a nod to privacy concerns, they are primarily concerned with technical issues, such as interoperability across branches, identifying

---

13 U.S. Navy. "X-47B Operates Aboard Theodore Roosevelt," news release, November 10, 2013, http://www.navy.mil/submit/display.asp?story_id=77580.

14 Department of Defense, *Unmanned Systems Roadmap 2007–2032* (Washington, DC: Department of Defense, 2007), 62.

15 U.S. Air Force. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047* (Washington, DC: USAF Headquarters, May 18, 2009), 3.

16 Ibid.

17 U.S. Army. *U.S. Army Unmanned Aircraft Systems Roadmap 2010–2035* (Fort Rucker, AL: U.S. Army Center of Excellence, 2010).

future requirements, testing new models for different uses, and planning for future technology integration.

3. Law Enforcement

To a much lesser extent, local law enforcement agencies have started experimenting with UAS. Some of these efforts—such as in Seattle—were halted to allow lawmakers to catch up with the technology. Anticipating a surge in law enforcement uses, the International Chiefs of Police (IACP) Aviation Committee published a concise three-page guide for law enforcement use of UAS in August 2012. Although short, the guide touches on critical issues ranging from public engagement to technical recommendations.[18]

4. Other Government Agencies

In addition to its own high-altitude UAS research, NASA is holding an Unmanned Aircraft Systems Airspace Operations Challenge to encourage the development of safety related UAS technology, such as sense and avoid and lost communications link systems.[19] Also, as noted earlier, Customs and Border Protection acquired several large UAS to assist with border patrols and other efforts in support of emergency services.

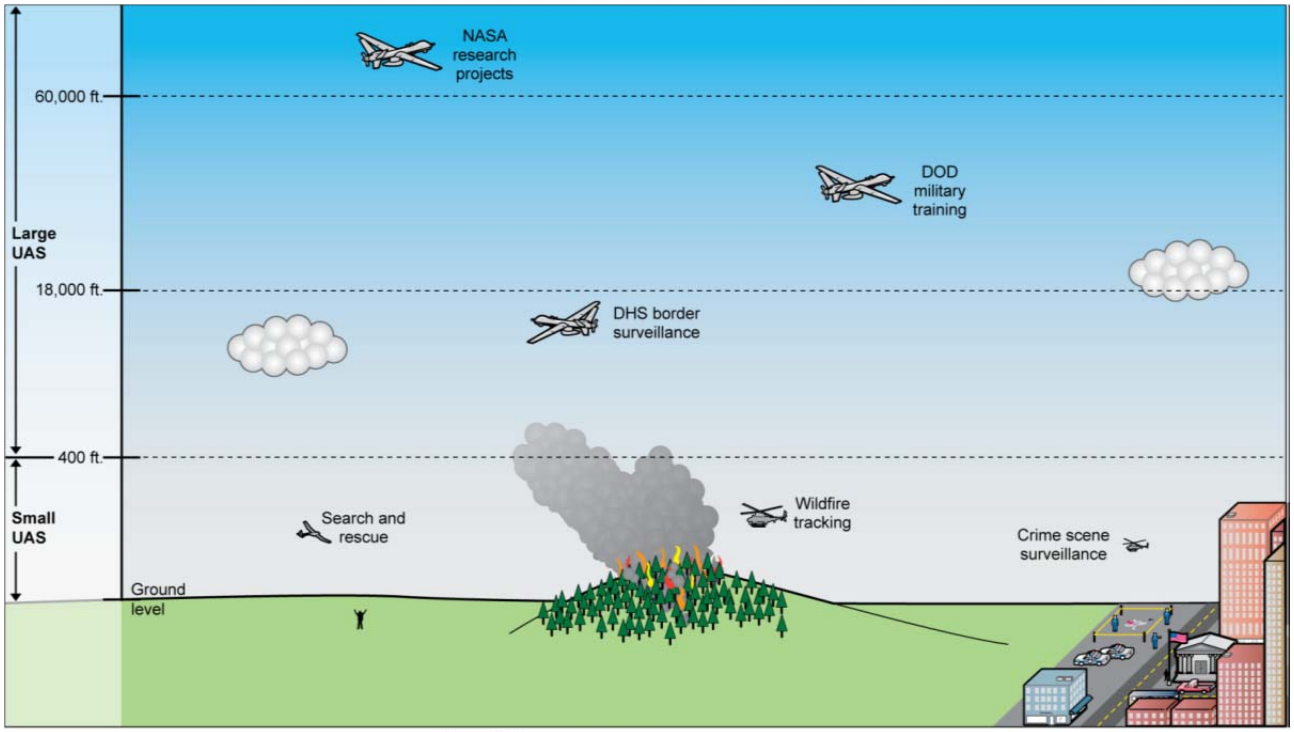
Figure 2 provides a relatively current snapshot of the possible uses of UAS in national airspace, although it does not include hobbyist and other nonsanctioned UAS, nor is it updated to include the UAS test sites.

Figure 3 shows a sample of the variety of sizes and shapes that a UAS can take, ranging from a device that can fit in the palm of one's had to high-altitude airframes with a wingspan close to 100 feet.

---

18 "Recommended Guidelines for the Use of Unmanned Aircraft," International Association of Chiefs of Police Aviation Committee, accessed August 16, 2013. http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

19 "Unmanned Aircraft Systems Airspace Operations Challenge (UAS AOC)," NASA, accessed January 6, 2014. http://www.nasa.gov/directorates/spacetech/centennial_challenges/uas/index.html#.UuWVStLTnDc.



Source: GAO.

Figure 2. Examples of Current Uses for UAS and their Altitudes of Operation..[26]

[26] Gerald L. Dillingham, *Unmanned Aircraft Systems, Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, GAO-12-981(Washington, DC: GAO, Government Accountability Office, 2012), 6.

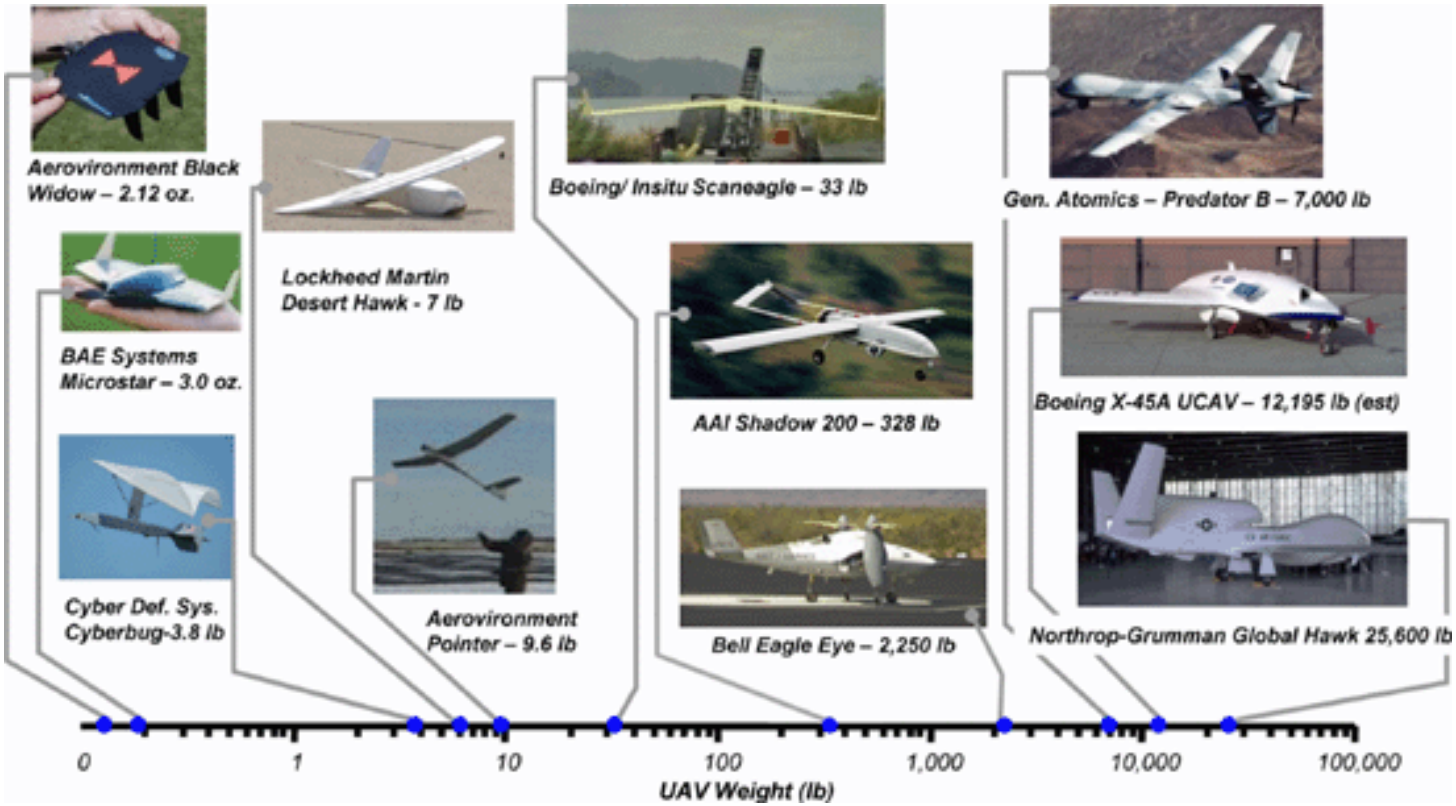
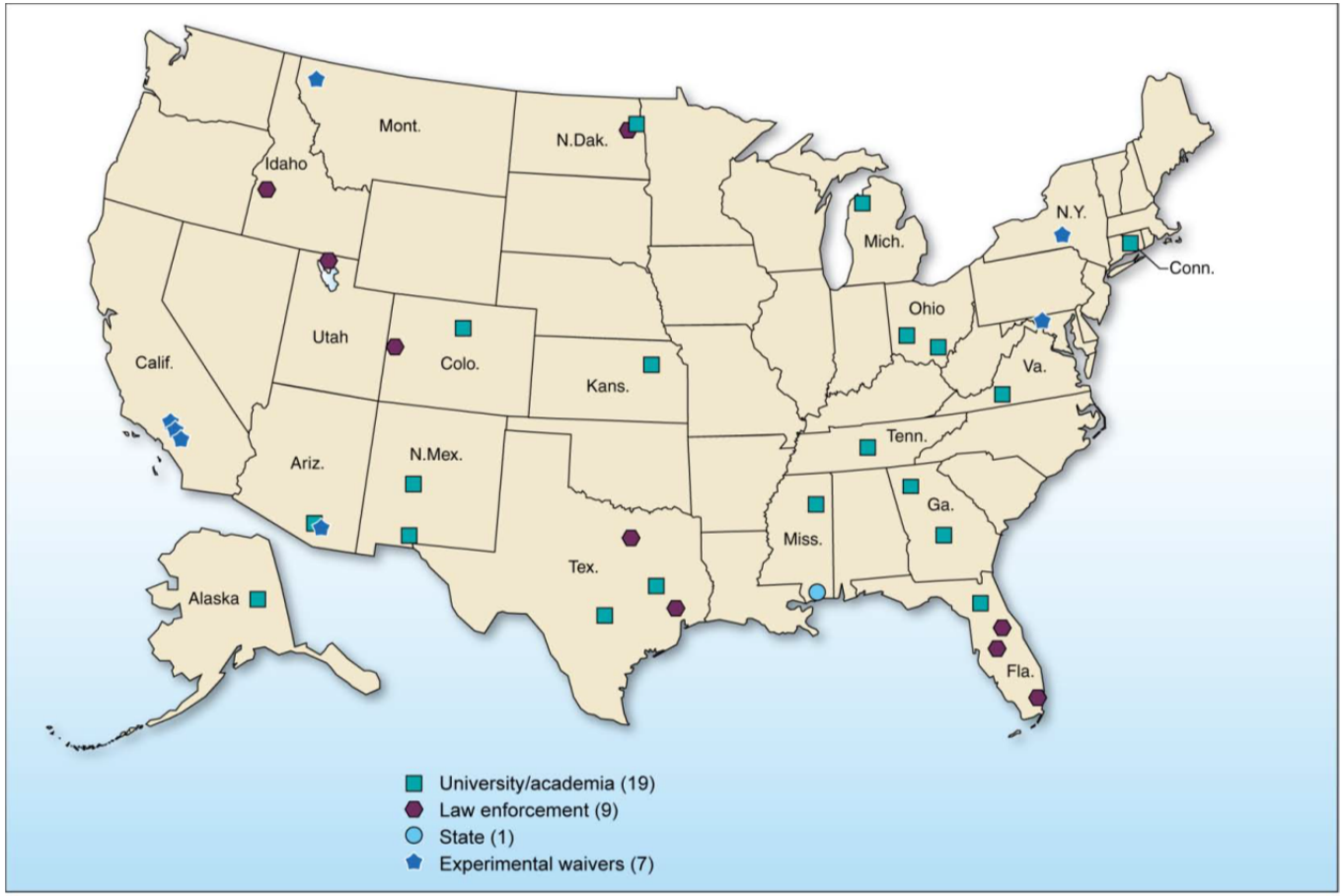


Figure 3. Sample of Unmanned Systems[27] https://ieeexplore.ieee.org/ieee_pilot/articles/96jproc12/jproc-RWeibel-2006118/article.html

[27] Aleksandra L. Mozdzanowski et al., "Feedback Model of Air Transportation System Change: Implementation Challenges for Aviation Information Systems," *Proceedings of the IEEE* 96, no. 12 (2008): 1977–1978. https://ieeexplore.ieee.org/ieee_pilot/articles/96jproc12/jproc-RWeibel-2006118/article.html.



Sources: FAA and Map Resources.

Figure 4. NonFederal Recipients of Certificates of Waiver or Authorization and Special Airworthiness Certificates in the Experimental Category and the Location, as of July 13, 2012.[28]

[28] Dillingham, *Unmanned Aircraft Systems*, 6.

Figure 5. Selected UAS Test Site Operators[29]

[29] "Unmanned Aircraft Systems (UAS) Infographic," Federal Aviation Administration, accessed January 2, 2014. http://www.faa.gov/about/initiatives/uas/infographic/.

5. Opportunity, Controversy and the Great Unknown

UAS proponents have strong support through the Congressional Unmanned Systems Caucus in the U.S. House of Representatives. From the industry perspective, the nation is on the verge of a new era in aviation. The industry voice is represented through The Association for Unmanned Vehicle Systems International (AUVSI), a global advocacy network with 2,500 member organizations representing 7,000 members from government industry and academia across 55 allied countries. This group strives for broad adoption of UAS across society.

However, there are a number of issues driving the debate over UAS use, led by civil liberties and safety concerns. The American Civil Liberties Union (ACLU) and the Human Rights Watch are two leading voices of dissent, warning of the negative potential of widespread UAS use, rather than actual usage. (Of note, neither organization advocates that UAS be abolished, rather, they advocate for cautious implementation, public and congressional oversight and nonlethal use.)

Anticipating a surge in UAS use to fight crime, the ACLU and other civil liberties advocates base their opposition on the possibility that unmanned aircraft in national airspace could launch the nation into an era in which the government increasingly invades individuals' privacy to collect data on the noncriminal activities of ordinary Americans.[30]

a. Accelerating Technology

Although not a new technology, UAS in the domestic airspace are a disruptive technology. Clayton Christensen, who coined the term in his book The Innovator's Dilemma, describes how well-established industries can be disrupted when they focus on sustaining existing ways of doing business through incremental change. A disruptive technology is one that may only have a niche market to begin with, may be cheaper and

30 "Domestic Drones," American Civil Liberties Union Blog of Rights, accessed February 3, 2013. https://www.aclu.org/blog.To prevent a "surveillance society" from developing, the ACLU has drafted recommended guidance, which is integrated in recommendations at the end of this thesis.

have limited utility, but which rapidly and radically changes the market, ultimately leaving the traditional competitor in the dust.[31]

Technology is advancing far faster than a bureaucracy can pass sensible laws to manage the consequences. In addition to civil liberties issues that must be addressed, basic safety concerns can be compounded as technology rapidly outpaces the government's ability to regulate it. There are even psychological consequences of a rapid change, when changes on a macro level are taking place faster than humans can adapt psychologically.[32]

b. Autonomy

Anyone with a Roomba vacuum cleaner or an automatic pool vacuum is already familiar with autonomous robots. At present, UAS are actually fairly large systems requiring a support team, composed of an operator and often a larger crew to support communications and maintenance, depending on the size and purpose of the UAS. However, autonomous capability is being developed for UAS, which will eventually allow pre-programmed UAS to conduct activities without a human operator monitoring and guiding the vehicle from another location. This could be very useful in particularly dull jobs, such as monitoring pipelines or surveying crops.[33]

Foreseeing the development of completely autonomous UAS in the near future, in its report, *Losing Humanity: The Case Against Killer Robots*, the Human Rights Watch calls for an internationally binding law that would make it illegal to arm an autonomous UAS (a UAS that is programmed with certain parameters and then set free to conduct its activity without human decision makers' input.)

Daniel Suarez, author of "Kill Decision," also makes a compelling case against autonomous armed robots in the 2013 Ted Talks discussion, "The Kill Decision

---

[31] Clayton Christensen, *The Innovator's Dilemma* (New York: HarperBusiness, 2000).

[32] Fathali M. Moghaddam, "*From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*. Westport, CT: Praeger, 2006, 130.

[33] Even in the case of fully automated unmanned vehicles, a human being must enter the parameters at the outset. In essence, a UAS is simply an extension of the operator and his or her intent, and accountability could follow suit.

Shouldn't Belong to a Robot." He draws comparisons between feudal society and the evolution of the military and democracy, then links evolving technologies used for mapping out social connections with the potential for anonymous war. To avoid a dystopian future, he joins the Human Rights Watch call for an international treaty to make autonomous armed robots illegal. As a way to enforce accountability, Saurez suggests that "Each robot and drone should have a cryptographically signed I.D. burned in at the factory that can be used to track its movement through public spaces... And every citizen should be able to download an app that shows the population of drones and autonomous vehicles moving through public spaces around them."[34]

Civil liberties activists are concerned that dictators may use UAS against their own citizens.[35] They are also concerned about the "dehumanization" of weapons systems, claiming that a human being is more likely to show compassion and therefore less likely to kill. The Human Rights Watch and other human rights groups fear that as UAS become more and more autonomous, it will become easier to kill in circumstances where a normal human might hesitate. This line of thinking is illustrated in the *Lucifer Effect*, in which Stanford professor Phillip Zimbardo makes the case that de-personalizing a human makes it easier to do things that an ordinary person would never do under normal circumstances. In the infamous Stanford Prison Experiment conducted by Zimbardo in 1971 and later experiments, as well as during an examination of the prison abuses at Abu Ghraib, Zimbardo found that separating someone from their victim, whether through masks, distance or other depersonalizing techniques, also reduces inhibitions in such a way that an individual finds it easier to conduct illegal, violent or otherwise extremely anti-social behavior.[36] In his discussion on the "mechanisms of moral disengagement," Zimbardo says "we can minimize our sense of a direct link between our actions and its harmful outcomes by diffusing or displacing personal responsibility."[37] Civil rights

---

34 Daniel Suarez, "The Kill Decision Shouldn't Belong to a Robot," *Ted Talks*, posted June 2013. http://www.ted.com/talks/daniel_suarez_the_kill_decision_shouldn_t_belong_to_a_robot.html.

35 Human Rights Watch, *Losing Humanity: The Case Against Killer Robots*. (New York: Human Rights Program Watch, November 19, 2012).

36 Philip Zimbardo, *The Lucifer Effect: Understanding How Good People Turn Evil* (New York: Random House, 2008), 298–301, 324–325.

37 Ibid., 311.

activists are concerned that the distance and technological barriers between UAS operators and other humans could make it easier to use lethal force, if UAS are armed.

Conversely, in the NBCnews.com article, *Anticipating domestic boom, colleges rev up drone piloting programs*, Texas A&M computer science student Brittany Duncan suggests that a remote pilot is more likely to take more time to determine the threat before shooting, since they are not immediately threatened. (Duncan, a licensed pilot, is studying robot-human relations to see how robots might help disaster survivors.)[38]

c. Sensor Technology

A UAS is essentially a flying platform that can be equipped with a range of equipment, including highly sensitive cameras that can collect very detailed information from wide swaths of area—very useful in geographical surveys, for instance, but potentially also capturing information that the UAS operator was not seeking.

The September 2012 GAO report, *Unmanned Aircraft Systems, Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, notes privacy as an emerging concern as sensor technology is increasingly capable of collecting massive amounts of data.[39] A Congressional Research Service (CRS) report also released in 2012, *Drones in Domestic Surveillance Operations Fourth Amendment Implications and Legislative Responses*, observes that advanced sensor technology will also draw a focus to law enforcement issues like curtilage and open fields—two legal measures of private and public space—as UAS and their sensor payloads provide ever more defined insight into back yards and even into buildings.[40] .

---

[38] Rafter, "Anticipating Domestic Boom."

[39] Dillingham, *Unmanned Aircraft Systems*, 32–36.

[40] Richard M. Thompson, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Respo*nses, CRS Report R42701(Washington, DC: Library of Congress, Congressional Research Service, April 3, 2013, 7, 16.

d. Privacy

The U.S. population is uniquely protective of its privacy compared to other democratic nations like the U.K., which regularly uses CCTV for surveillance in public spaces. Implicit protections for individual privacy are embedded in the U.S. Constitution through the 4th Amendment.

The ACLU and other civil liberties advocates believe that unmanned aircraft in civil airspace could launch the nation into an era in which domestic surveillance increasingly captures the noncriminal activities of Americans.[41] To prevent the U.S. from sliding into a "surveillance society," the ACLU has drafted recommended guidance in *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft.*[42] Key concepts from this report are integrated in recommendations at the end of this paper.

e. Legal Frameworks

The privacy issue is complicated. There is no single, overarching privacy law that can be applied nationwide; instead there is a hodge-podge of federal, state and local laws that can vary significantly. Many people point to the 4th Amendment as the source of a "right to privacy." However, this protection is not explicit, nor does it address modern technology: the Fourth Amendment was established after the American Revolution to protect Americans from "unreasonable search and seizure" and requires probable cause and a warrant. It states very briefly:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[43]

---

[41] Jay Stanley Crump and Catherine Crump. *Protecting Privacy from Aerial Surveillance*. (Washington, DC: American Civil Liberties Union, 2011), 1.

[42] Crump, *Protecting Privacy*, 15–16.

[43] *United States Constitution, The Bill of Rights*, accessed January 11, 2014, http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

Other federal laws include the Privacy Act of 1974 and the E-Government Act of 2002. The Privacy Act limits government collection and use of personal information in public records, while Section 208 of the E-Government Act adds a requirement for agencies to conduct Privacy Impact Assessments prior to collecting personally identifiable information like names, contact information, and social security numbers..[44] Specifically, Section 208 states that the intent is to "ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government."[45]

Notably, neither of these laws provides general protection from surveillance in public spaces, such as might be conducted by traffic cameras, police aircraft, neighborhood drive-bys or other law enforcement activities to monitor criminal activity.

f. Safety

While not the primary focus of this thesis, it is worth commenting on the safety issues that must be considered when integrating UAS into domestic air space. Air traffic is strictly controlled by FAA regulations; pilots must file a flight plan before travelling, and must stay in contact with air traffic control in the event that course adjustments must be made. However, there are no established regulations for unmanned flight; moreover, unmanned aircraft systems (which include the remote operator) have potential vulnerabilities that are still being explored. The Air Line Pilots Association (ALPA) published a white paper in April 2011 stating its position that "no UAS should be allowed unrestricted access to public airspace unless it meets all the high standards currently required for every other airspace user."[46] After the Customs and Border Protection (CBP) drone was flown into the sea off the California coast in January 2014, ALPA again voiced its concerns over the need to prioritize safety as UAS integration moves forward.

---

[44] Dillingham, *Unmanned Aircraft Systems*, 34.

[45] Electronic Privacy Act of 2002, Pub. L. No. 107–347, 116 Stat. 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf .

[46] Air Line Pilots Association, *Unmanned Aircraft Systems: Challenges for Operating Safely in the National Airspace System*, White paper (Washington, DC: Air Line Pilots Association, 2012).

In the February 2013 WFAA news article, *Arlington police hopeful their drones will soon be taking flight*, some commercial pilots expressed their lack confidence in the current level of "see and avoid" technology, and fear that UAS pose a safety risk to manned aircraft- especially if the operator loses communication with the UAS.[47] However, "sense and avoid" technology is under development be several agencies, including NASA.

g. Market Competition

Although UAS have been in use since at least the early part of the 20th century, they could be considered a disruptive technology within the context of national airspace. Harvard professor and author Clayton Christensen coined the term, which he describes in *The Innovators Dilemma*. Essentially, a disruptive technology is something that starts with a niche market, with simpler, lower cost solutions, and then quickly displaces more expensive traditional technologies. Examples include the introduction of the Model T Ford, desktop computers and cell phones.

The appetite for adapting UAS capability to domestic use has grown rapidly in both the public and commercial sectors, already outpacing legal considerations. The potential cost savings of UAS is inviting to strapped law enforcement agencies that want to use UAS to monitor and fight crime; homeland security agencies like Customs and Border Protection have already started using UAS on a limited basis to patrol large, and largely unpopulated, U.S. borders, conduct search and rescue missions and even assist firefighting. There is also vast potential for commercial use, ranging from monitoring gas pipelines and other critical infrastructure, to film-making, agriculture and cargo.

UAS proponents have strong support through the 50-member, bipartisan Congressional Unmanned Systems Caucus—although the Caucus appears to be primarily interested in promoting UAS for military and defense use. From the industry perspective, the nation is on the verge of a new era in aviation. Aerospace companies are anticipating new growth markets and an NBCNews.com article, *Anticipating domestic boom, colleges*

[47] Monica Diaz, "Arlington Police Hopeful Their Drones Will Soon Be Taking Flight," *WFAA News*, February 7, 2013, http://www.wfaa.com/news/local/tarrant/Arlington-police-hopeful-their-drones-will-soon-be-taking-flight-190325001.html.

rev up drone piloting programs, discusses why a handful of colleges are already creating degree programs for UAS operators.[48]

h. Cybersecurity

Concurrent with the rise of UAS is a growing awareness of the inherent vulnerabilities in technology that relies on the Internet although not widespread at present, it is possible for UAS sensors and guidance systems to be hacked, as in the case of the RQ-170 drone that was captured in Iran.

6. Summary

Since beginning this research, additional literature has been generated at an exponential rate, especially in the press. Current events such as targeted drone strikes on U.S. citizens overseas, the Edward Snowden leads on National Security Agency surveillance, and FBI use of drones in America have raised public concerns and a greater demand for public discussion on the issue. Congress is scrambling to draft legislation to address privacy issues, and universities are scrambling to put together courses on "drone journalism" and UAS operation. Yet, the technology and the global markets for it are evolving so quickly that any attempt to legislate it seems to lag ever further behind.

In an attempt to mitigate concerns like these, the UAS industry itself has proposed what it calls "common sense" guidelines for the growing international community of UAS researchers and users. These guidelines are posted on the organization website, http://www.auvsi.org/conduct, and rest on the core principles of "safety, professionalism and respect"[49]

A growing number of other organizations have also contributed proposals for UAS policies as well, notably privacy and civil liberties advocates. As UAS integration takes a more prominent place in public discussion, this thesis will attempt to orient

---

[48] Rafter, "Anticipating Domestic Boom."

[49] "Unmanned Aircraft System Operations Industry 'Code of Conduct,' " Association for Unmanned Vehicle Systems International, accessed February 2, 2013. http://www.auvsi.org/conduct.

homeland security practitioners and interested observers to some of the key issues that should be considered.

E. OVERVIEW OF CHAPTERS

Although there are a number of intriguing challenges rising out of the UAS debate, the privacy issue seems to be the biggest and most difficult to wrangle into place. Safety issues have a fairly clear line of ownership back to the FAA, but no single entity "owns" the privacy issue.[50] However, privacy issues leave their mark across technology, law, and that most nebulous and unpredictable of all things: human emotions.

With privacy as the context, the following chapters provide an introduction to some key considerations for homeland security practitioners or emergency managers who are considering UAS as a means to augment their capabilities.

- These start with a discussion of how people react to change and risk, to provide a foundational understanding of how the U.S. population might react to UAS integration.
- The next chapter is an orientation to the political-economic landscape of stakeholder groups and their potential interests in the issue, all of which should be considered as a jurisdiction plans how and when to introduce UAS to its community.
- A chapter on cybersecurity touches on an emerging issue that will impact privacy and security as UAS become more common in a nonmilitary role.
- The social and legal framework for privacy and civil liberties are addressed at length in the following chapter, including a look at how the United Kingdom and European Union approach privacy issues and technology.
- The thesis concludes with thoughts on future considerations, along with analysis and recommendations drawn from the various organizations that have started to develop proposals for addressing privacy.

[50] The lack of ownership and accountability of widely used resources, such as the Internet, is also described as the Tragedy of the Commons.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RADICAL CHANGE, RISK AVERSION AND THE TRIUMPH OF PUBLIC OPINION

Although UAS have been used by the military since the early part of the 20th century for training and, more recently, surveillance, until very recently they have been separated from mainstream America physically and cognitively. Now, with the advent of domestic use for UAS, the public is faced with a change that some might compare to the introduction of the automobile in the early 1900s,[51] in that mainstream America may very well see a radical technological evolution in a very short amount of time. While some early adopters eagerly embraced the horseless carriage, the newspapers of the period have numerous articles expressing public outrage over these dangerous, nuisance-y machines.

With the introduction of UAS, many more unknowns enter into the mix than during the introduction of the automobile, notably thanks to the ability of UAS to go almost anywhere and their ability to carry equipment that can capture large amounts of highly detailed visual data. The issue is also greatly confused by the growing public awareness of military drone usage, along with the media coverage of alleged NSA surveillance.

Even as press started increasing its scrutiny of NSA spying and military drones in the interest of public debate, Amazon CEO Jeff Bezos announced his plans to test small UAS for commercial delivery.[52] Weeks later, on December 30, 2013, the FAA announced six competitively selected UAS test sites around the U.S., as required in the FY 2012 FAA appropriations act. These two announcements spurred a flurry of media stories anticipating technological evolution along with growth opportunities for industry and employment. In a curious juxtaposition to relatively neutral or positive mainstream media coverage, online discussion following these articles was quite negative.

---

[51] Peter Singer, "The Predator Comes Home: A Primer on Domestic Drones, Their Huge Business Opportunities, and Their Deep Political, Moral and Legal Challenges," *Brookings Institute*, March 8, 2013. http://www.brookings.edu/research/papers/2013/03.08-drones-singer.

[52] Manjoo Farhad, "Why Bezos's Drone Is More Than a Joke," *Wall Street Journal*, last modified December 5, 2013. http://online.wsj.com/news/articles/SB10001424052702303722104579238312058025896.

For example, the commentary following a December 30, 2013, CBS news article[53] offers overwhelmingly negative opinions, often referencing dystopian movies like *Terminator* or *Robocop*. One comment from "JamesBrains" states:

> I'd be okay with this if I could trust the government and big business. Of course, I can't. All it takes is a bomb here or there in the U.S., and all of a sudden, every branch of the federal government is fine with drones spying on every [expletive] American (if they aren't already). (December 30, 2013 7:7PM)

Interspersed with rare comments take a positive stance on the issue, other messages respond with threats to capture or shoot down any drones that fly over their property. This comment by "ToddWest" is captures typical concerns expressed in online conversations about government or corporate usage:

> @wstcstmsgrthe IRS or anyone else starts flying devices over my property and keeping the a/v on file to build a dossier on me I will take it as acts of war against me....the government is a massive criminal organization, I am not interested in the benefits of kneeling down to such a beast. (December 30, 2013 1:1PM)

Are these just random ravings, or do they accurately capture public sentiment? According to at least two studies,[54] the public would generally be in favor of using UAS for emergency management or homeland security. However, those same studies also indicated a relatively low awareness of UAS overall, meaning that a large portion of the population is undecided and potentially could be persuaded in either direction. With the media magnifying both the pros and cons of UAS integration, how might public opinion be swayed?

To understand how people react to the prospect of massive change on the scale of what America faces now, two theories can provide context: prospect theory, as discussed in Daniel Kahneman's book *Thinking Fast and Slow*, and the Macro-Micro Rule of

---

[53] "FAA Announces Drone Testing in Six States," Associated Press, December 30, 2013.

[54] Monmouth University, *National: U.S. Supports Unarmed Domestic Drones But Public Prefers Requiring Court Orders First* (West Long Branch, NJ: Monmouth University, August 15, 2013) https://www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/409aecfb-3897-4360-8a05-03838ba69e46.pdf; Joe Eyerman et al., *Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns* (Research Triangle Park, NC: Institute for Homeland Security Solutions, 2013).

Change, introduced by Georgetown professor Fathali M. Moghaddam in *From the Terrorists' Point of View*.

A. PROSPECT THEORY (RISK AVERSION)

If one can assume that opening up national airspace to UAS is something of a gamble— in other words, there is no way to know where this technology will take the U.S. over time—then prospect theory offers a solid framework for understanding potential public reaction to such uncertainty.

Kahneman won a Nobel Prize in economic sciences in 2002 for demonstrating that people are inherently biased toward risk aversion when making decisions with uncertain outcomes. According to prospect theory,[55] most people prefer to keep what they know rather than risk losing something they have- even if there a greater likelihood of attaining an even greater benefit if they take the risk. Kahneman also discusses how negativity dominance can impact decision making, claiming that this is a survival mechanism.

"The brains of humans and other animals contain a mechanism that is designed to give priority to bad news," says Khaneman. "Loss aversion is a powerful conservative force that favors minimal changes from the status quo in the lives of both institutions and individuals. This conservatism helps keep us stable in our neighborhood, our marriage, and our job; it is the gravitational force that holds our life together near the reference point."[56]

1. Micro-Macro Rule of Change

It is also possible to apply Fathali Moghaddam's Micro-Macro Rule of Change to the integration of UAS in domestic airspace. Moghaddam, an expert in psychology and terrorism, explains that there is a deep psychological disconnect between the rate of change at a macro, or political-economic level, and the micro level of individual. In other words, a change introduced relatively quickly on a society-wide basis may take a much

---

[55] Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux), 283–286.

[56] Ibid., 305.

longer time to absorb on an individual basis as individuals have to adjust to dramatically new circumstances. If this rule were applied to the introduction of UAS, then it could be assumed that the U.S. population would need time to acclimate themselves psychologically to dramatic new changes that could come with UAS use.

2. Easing the Transition

In a 2013 survey of more than 2,000 U.S. residents nationwide, the Institute for Homeland Security Solutions found that the 44 percent of respondents reported little or no prior awareness of domestic uses for UAS. However, over half of respondents supported the use of UAS for protecting life and property as well as for commercial use. Key concerns included possible monitoring, safety and the government's ability to regulate UAS. All of these concerns scored very high, in the 65–75 percentile.[57] These concerns and the large percentage of undecided opinion could indicate an opportunity to move public opinion for or against UAS. Active, ongoing public engagement is key to fostering public acceptance of domestic UAS. This is discussed in the next chapter.

[57] Joe Eyerman et al., *Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns* (Research Triangle Park, NC: Institute for Homeland Security Solutions, 2013).

III. STAKEHOLDER ENGAGEMENT

Communications professionals understand that in the absence of information, people will fill in the blanks with their own version of the truth. With such a diverse collection of entities and coalitions actively shaping the environment within which the UAS debate is growing, it is important for all who are considering UAS to understand how differing agendas can influence the picture.

Figure 6 offers a high-level snapshot of the various interest groups and factors that influence their motives. As can be seen in the graphic, the stakeholder landscape is fairly complex and nuanced. Some stakeholder groups, such as the federal government, must answer to groups with greatly varying agendas. Figure 7 shows the geographical spread of congressional interest in UAS, as well as the six FAA-approved test sites. Of interest, while there is significant geographical spread, there are also wide stretches of the country with no representation and no test site. Without further research it is difficult to assign a level of significance, but it may indicate sections of the country with comparatively little awareness of the coming UAS integration.

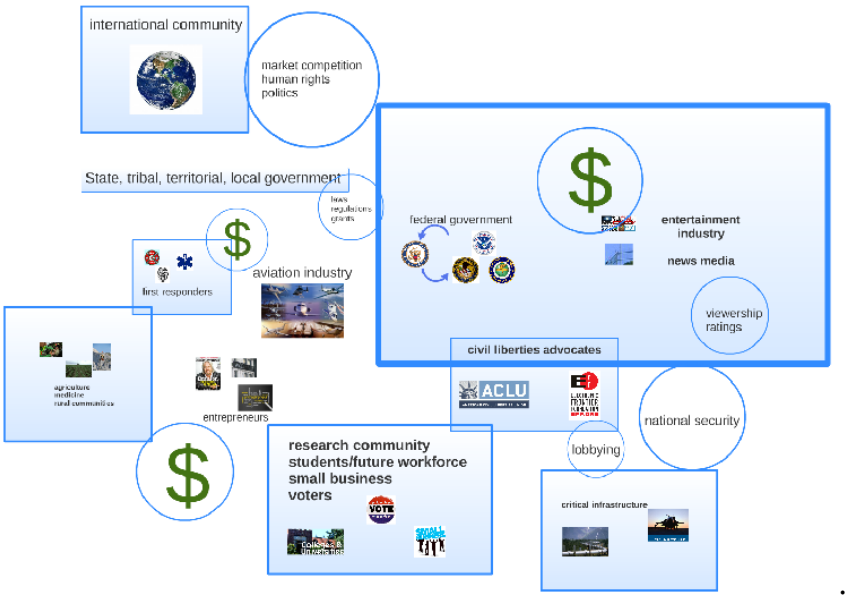


Figure 6. Conceptual Map of Stakeholders with an Interest in UAS in American National Airspace and Influencing Factors

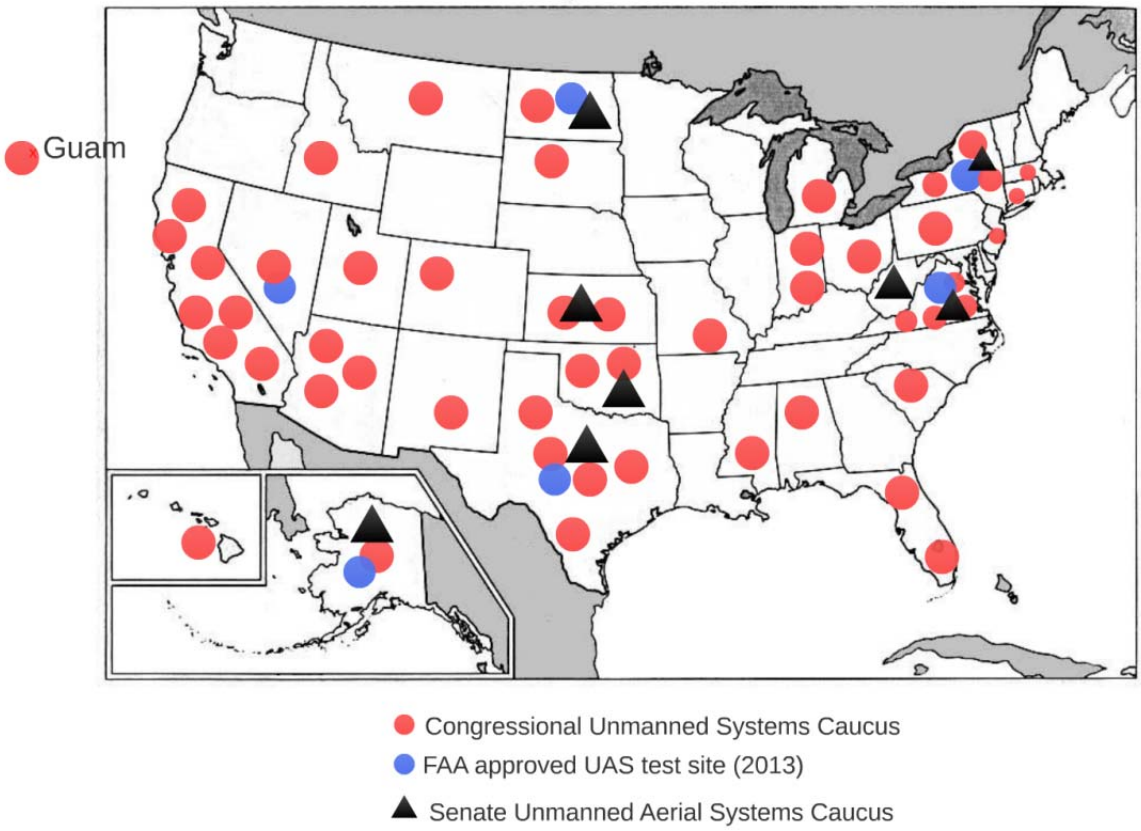


Figure 7. Map of Congressional Representation on Senate and House UAS Caucuses, Overlaid with the Six FAA-Approved UAS Test Sites as of December 31, 2013.

A. STAKEHOLDER GROUPS

1. Federal

Congressional Unmanned Systems Caucus (U.S. House of Representatives: Co-chaired by Buck McKeon (CA-25) and Henry Cuellar (TX-28), this 50-member committee was formed explicitly to promote the use of UAS. Its mission is "educate members of Congress and the public on the strategic, tactical, and scientific value of unmanned systems; actively support further development and acquisition of more systems, and to more effectively engage the civilian aviation community on unmanned system use and safety."[58]

[58] "Congressional Unmanned Systems Caucus," Unmanned Systems Caucus, accessed January 14, 2014. http://unmannedsystemscaucus.mckeon.house.gov/about/purpose-mission-goals.shtml.

Senate Unmanned Aerial Systems Caucus: This 8-member committee was formed in 2012 to work on the privacy and other issues related to UAS.[59] It has no website and as yet there is little information on the caucus beyond what was available in a press release. However, its presence indicates a growing awareness and interest in the issue on the other side of Congress.

Department of Homeland Security: The Department's mission includes "preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience."[60] Interest in UAS might include support for monitoring the nation's extensive borders to disaster damage assessments or search and rescue.

Federal Aviation Administration: The FAA received a congressional mandate in the FY 2012 appropriations to develop rules that would allow UAS to fly in domestic airspace by 2015. Its mission is to "provide the safest, most efficient aerospace system in the world."[61] The FAA's primary interest in UAS will be focused on safety issues.

National Aeronautical and Space Administration (NASA): NASA is developing high-altitude UAS for scientific exploration, and they have issued a private sector challenge to find solutions to technical issues related to safety, such as improved sense and avoid technology.

2. State, Local, Tribal, Territorial (SLTT)

Homeland security and emergency management offices: All levels of government will need to understand the possibilities and issues related to UAS, as they determine whether to spend diminishing funds on acquiring these systems.

---

[59] Yasmin Tadjdeh, "New Senate Unmanned Aerial Vehicle Caucus to Tackle Privacy Issues," *National Defense Magazine*, December 2012, http://www.nationaldefensemagazine.org/archive/2012/December/Pages/NewSenateUnmannedAerialVehicleCaucustoTacklePrivacyIssues.aspx.

[60] "Mission," Department of Homeland Security, accessed January 2, 2014, http://www.dhs.gov/mission.

[61] "Mission," Federal Aviation Administration, accessed January 2, 2014, http://www.faa.gov/about/mission/.

First responders: Law enforcement, fire and other emergency responders may have a strong interest in UAS technology as economically viable way to bolster teams that are already spread thin.

3. Commercial

Aviation: The aviation industry faces significant disruption with the advent of UAS. New technology may be needed to operate manned and unmanned aircraft safely in the same space. UAS technology can also be integrated into traditional aircraft to improve safety and reliability of human-piloted airplanes.

Agriculture industry: UAS equipped with the right sensors can monitor and help manage water and pest conditions, saving water and crops.

Critical infrastructure owners and operators: The nation relies on tens of thousands of miles of electrical transmission lines, gas pipelines, and other critical infrastructure that is often located in remote areas. UAS could offer cost effective ways to monitor, repair or protect this infrastructure.

Defense industrial base: Large corporations that have traditionally developed aerospace products for the Department of Defense may be interested in developing new markets at home, as budgets for foreign wars are scaled back.

Entrepreneurs: Entrepreneurs will find opportunities to exploit the potential of UAS in creative ways.

Entertainment: Hollywood, sporting events and paparazzi are all potential customers, as UAS offer new ways to get close to the action.

Shipping companies: With Amazon the first to set its flag in the sand, other shipping companies are likely to start exploring the potential for cheaper ways to transfer cargo.

4. Interest Groups

Media: As the traditional public watch dog and as a business interest, the media will be interested in any stories about UAS that will sell readership/viewership. However, the media is also a critical information channel and should be engaged early and often to help educate the public and facilitate a public dialogue on the issue.

Activists: Civil liberties groups, privacy advocates, environmental groups and other public interest organizations will be concerned with potential negative consequences of UAS integration.

Pilots: Traditional pilots may feel threatened by the potential loss of aviation careers. They may also be concerned about safety issues related to communicating with and flying near UAS. According to a Bloomberg news article on the January 2014 Customs and Border Protection (CBP) Predator crash off the coast of California, the Air Line Pilots Association (ALPA) called for the FAA to reconsider its timeline for UAS integration in order to give safety issues and regulations more time to be resolved. (CBP grounded its remaining fleet of nine drones- at least until the cause of the mechanical failure could be determined.)[62]

Individuals: Homeowners and other individual citizens may approach the UAS from any number of perspectives, ranging from "not over my back yard," to "how soon can I get a UAS to augment my home security system."

5. Academia

Scientific and engineering communities: The scientific and engineering communities will have the challenge of overcoming safety issues related to UAS and supporting the resolution of privacy and cybersecurity concerns. They will also play a key role in research and development as UAS applications evolve.

Academic and research institutions: Higher education institutions are already started to develop curricula for UAS pilots and UAS journalism. Research institutions

---

[62] Alan Levin and Jeff Plungis, "Pilots Say Go Slow on Commercial Drones after Ditching," *Bloomberg*, January, 29, 2014, http://www.bloomberg.com/news/2014-01-28/customs-drone-fleet-grounded-after-predator-goes-down.html.

straddle science and academia and will be important partners in UAS testing and development.

6. Illegal and Gray Areas

Drug runners, terrorists and other illicit enterprises: Often entrepreneurial themselves, drug runners are already using UAS to transfer products across borders. Terrorists are another form of entrepreneur, who might leverage UAS for surveillance and carrying cargo or might simply hack into legitimate UAS for nefarious purposes.

Paparazzi: Without firm legal guidelines, UAS offer paparazzi new ways to intrude on celebrities private lives.

B. SUMMARY

Stakeholder engagement plays a key role in successfully implementing change, and no less so in the area of UAS integration.

The IEEE, whose "core purpose is to foster technological innovation and excellence for the benefit of humanity," published a comprehensive technical paper in 2008, discussing change models for implementing new technology in national airspace, including UAS. The paper stressed the importance of stakeholder feedback as a part of the process and provided a diagram (Figure 8) that shows the role of stakeholder engagement and feedback in the change process.[63]

[63] Mozdzanowski et al., "Feedback Model of Air Transportation."

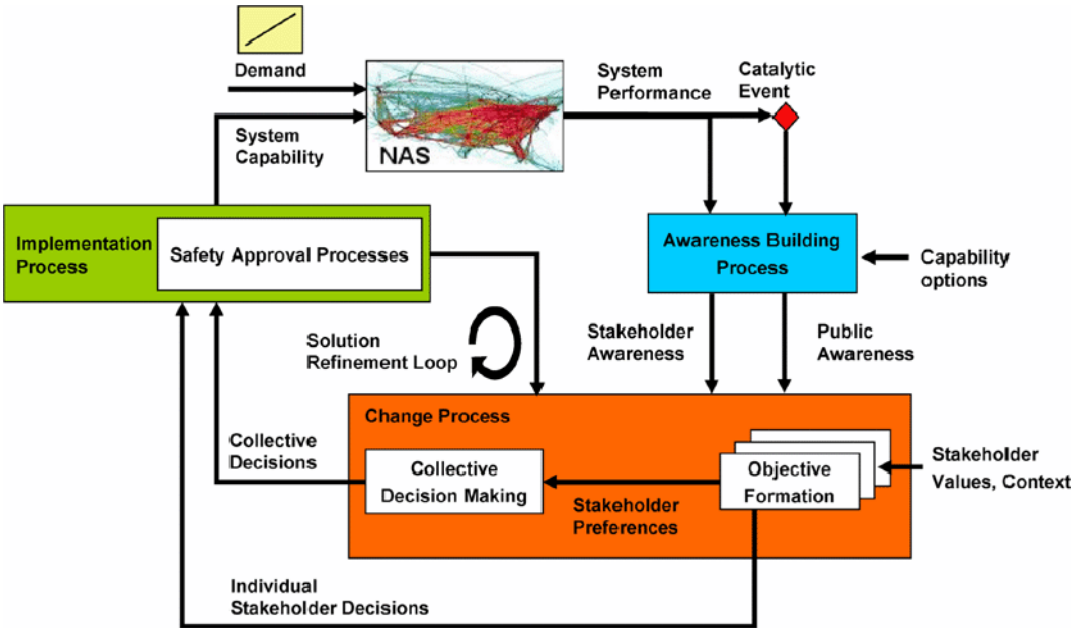


Figure 8. Change Dynamics Process Model.[64]

There is enormous political and market pressure by a coalition of global industry and congressional members pushing to integrate UAS into commercial and civil use. A widely cited study by the Teal Group[65] estimates the potential global industry to be worth $85 billion by 2020. It is easy to see why. Not only does language in the FAA's FY 2012 appropriations support widespread use of UAS for nonmilitary applications in the U.S. by September 2015,[66] but the economic accessibility of UAS is also likely to appeal to local law enforcement and emergency responders across tens of thousands of U.S.

In spite of this optimism, the prospect of American skies filled with drones raises alarms with civil liberties advocates who fear a pervasive intrusion by government into the lives of law-abiding citizens. First responders, on the other hand, might claim that UAS are simply a more economical platform for sensors that are already in use—and, in a way, they could be compared to airborne stoplight cameras. Regardless, the political tension surrounding the pending integration combined with negative media coverage of

[64] Ibid.

[65] Teal Group, "Teal Group Predicts Worldwide UAS Market Will Total $89 Billion."

[66] FAA Modernization and Reform Act of 2012, Pub. L. No. 12–95, 126 Stat. 11.Section 332 creates a mandate for the FAA to develop rules and pilots sites to integrate UAS into domestic airspace by 2015.

military drone strikes, Snowden and the NSA makes it all the more important that key issues are addressed promptly. Failure to do so could be catastrophic to the nascent domestic market.

In the face of these overwhelming and often opposing tensions, policy makers and the media must share the significant burden of establishing a strong, positive vision for where we, as a nation, want to go with UAS integration. Stakeholder engagement will be fundamental to shedding light on areas of concern and identifying an acceptable path forward.

IV. CONVERGING PATHS: CYBERSECURITY, UNMANNED SYSTEMS AND THE RISE OF TRANSPARENCY

Cybersecurity is an emerging issue that impacts every aspect of electronic life, from financial and other infrastructure networks, to online privacy and identify fraud. In his book, *America the Vulnerable, Inside the New Threat Matrix of Digital Espionage, Crime and Warfare*, former National Security Agency senior counsel Joel Brenner discusses the digital footprints that Americans create through GPS in their cars and smart phones, debit and credit card transactions, retail customer savings cards, social media and just about every other modern convenience—possibly soon to include UAS.

Many of these tools are now connecting with each other, creating an "Internet of Things" in which objects interact more efficiently with each other than with human operators. "We can't keep up with our own machines," Brenner writes. "so our machines have begun to talk to one another, making decisions for us, exchanging information about us" and doing everything from applying brakes to landing aircraft.

Moreover, as personal data proliferates and technology evolves exponentially,[67] Brenner laments "the law is chasing reality, not shaping it."[68]

This greater connectivity can also mean increased vulnerability, as attacks on one system can spread throughout the network. Not only can advertisers profile potential customers in great detail—thanks to software that connects the dots on all of our transactions—but organized crime, nonstate criminals, hackers, terrorists and foreign intelligence can just as easily exploit a myriad of weaknesses for their own means.

As a case in point, in June 2013, University of Texas at Austin professor Todd Humphreys took control of a UAS through a technique called GPS spoofing. Once he had control of the vehicle, he was able to divert it from its original course without raising any

---

[67] "Moore's Law or How Overall Processing Power Will Double Every Two Years," Moore's Law, accessed March 2, 2014, http://www.mooreslaw.org/.

[68] Joel Brenner. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press2011), 14–15.

alerts in the machinery or the authorized controller—again, similar to the tactic used by Iran in 2012.

Fortunately, Humphreys and the graduate students who assisted him were part of a team invited by the Department of Homeland Security (DHS) to test GPS spoofing on UAS in a controlled environment- in this case, on a type of UAS that is currently being marketed to law enforcement agencies. Humphreys had proposed the test to DHS as a way to identify and address potential security risks well before the FAA opens domestic airspace to commercial and civilian UAS in 2015.

Shortly after the experiment, on July 19, 2013, Humphreys testified before the House Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security. The hearing, called "Using Unmanned Aerial Systems within the Homeland: Security Game Changer?" drew on the expertise of witnesses ranging from law enforcement to privacy advocates and technical experts. In his written statement, Humphreys discussed the crucial difference between military GPS, which is secured and encrypted, and civilian GPS, which was designed to be open and accessible. The latter is highly susceptible to sabotage, and moreover, it is embedded into almost every mobile technology we use in daily life, from automobiles to commercial airlines to boats to mobile phones.

> The vulnerability of civil UAS to GPS spoofing is but one expression of a more fundamental problem: the insecurity of civil GPS signals. If a UAS can be hijacked by GPS spoofing, what else could go wrong within our GPS-dependent national infrastructure?[69]

Humphreys' questions refers to everything from transportation to communications to banking and finance to energy distribution infrastructure In the context of commercialized UAS, cybersecurity vulnerabilities threatens more than privacy; consequences of cyber-attacks can range from potentially massive economic losses from corporate espionage to hacking and sabotage through UAS networks and guidance

[69] *Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*: *Hearing Before the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland* Security, 112th Cong. (2012) (statement of Todd Humphreys of the University of Texas at Austin).

systems. According to Brenner, corporations—especially those specializing in industrial design, advanced technology (e.g., UAS) and pharmaceuticals- are increasingly targets of foreign and corporate espionage. Since the private sector produces UAS, along with most other products the country relies on already, UAS customers have to rely on the private sector vendors to maintain the integrity of the system.

Figure 9 shows a simplified concept of key points in the production timeline and corresponding cybersecurity threats, which is explained in more detail in the following section.

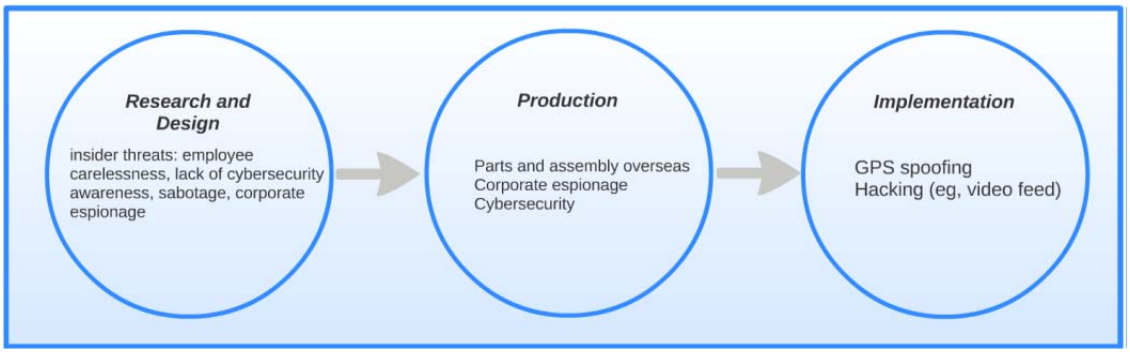


Figure 9. Cybersecurity Issues During UAS Production

Starting with the research and development process, corporate espionage and insider threats are among the top vulnerabilities. Other insider threats can be attributed to a critical lack of cyber awareness, disruption by disgruntled employees or even laziness on the part of employee or even top management—for example, moving a thumb drive from a personal computer to a business computer can open a company up to cyber exploitation.

The production cycle also offers numerous opportunities for sabotage. In *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, Brookings Institute Senior Fellow Peter Singer notes that "With the huge amount of 'civilian off the shelf' technologies used in military robotics, these trends actually create a massive dependence on foreign manufacturers to supply America's next generation of weapons. This

dependence has many worried "that foreign-made parts expose us to industrial espionage and cybersecurity threats."[70]

Although the focus of this research is on UAS in national airspace, rather than weaponized military drones, it can be assumed that the same market and supply chain issues would apply to commercially available UAS- if not more so. The efficiency and cost effectiveness of a global supply chain has created a world in which few, if any, vehicles (air, land or sea) are produced entirely within the U.S. While a UAS might be assembled in the U.S., the software, operating systems, sensors, and other physical components have likely been parsed out to vendors across the globe, including key "frenemies" and trading partners like China.

While China is not aggressively pursuing cyber-attacks on the military, it is dedicating considerable resources toward stealing industry technology and intellectual property. The key motive? Simply to ascend as a global economic power that can compete effectively with the U.S. and other first world countries. "China's motivation in this area is not mysterious," says Adam Segal in his *Foreign Affairs* article, "Chinese Computer Games: Keeping Safe in Cyberspace." "The government desperately wants its economy to move up the value chain, to become a source of innovation rather than just a producer of cheap goods."[71]

Once a UAS has moved into use, GPS spoofing becomes a growing concern. Moreover, moving back to the focus on privacy, hackers can potentially access data streams such as video and voice communications.[72]

---

70 Peter W. Singer, Wired for War: The Robotics Revolution and Conflict in the 21st Century, (New York: Penguin Books, 2009), 249.

71 Adam Segal, "Chinese Computer Games: Keeping Safe in Cyberspace," Foreign Affairs 91, no. 2 (March/April 2012):16.

72 Joel Brenner, America the Vulnerable, (New York: Penguin Press, 2011), 88-90. In his book, Brenner cites a case in 1996 where a U.S. Predator drone relied on unencrypted data links, allowing Iraqi opponents to watch real-time video of U.S. operations after hacking into the satellite feed.

A. PUBLIC AND PRIVATE SECTOR ROLES IN SOLVING CYBERSECURITY THREATS

Is the cyber threat significant enough that America should reconsider introducing UAS at home? While the threats are real, most of them lie in the realm of "possibility." Humphreys' test of GPS spoofing was conducted in a controlled environment with a highly skilled team. Lacking that level of expertise, Humphreys claims that widespread civilian GPS spoofing is "years away." Meanwhile, market competition is working. Corporations seeking to protect their future market are already advertising more secure data and GPS systems, and even alternatives to GPS, in industry publications like the Association for Unmanned Vehicle Systems International's member magazine, *Unmanned Systems*.

However, there is a question of whether industry will take a bare minimum approach to cybersecurity, or take a proactive stand. This is where, as Brenner notes, the customer base must leverage its buying power to demand higher standards of security at every weak point in the production and supply chain.

To overcome cyber threats to privacy and security in commercial UAS, there will need to be a collaborative effort between the public and private sectors. Together, federal government and private sector stakeholders must develop or select security standards for each of the known major vulnerabilities noted earlier, and then the government will need to provide regulatory oversight and leverage its buying power to force compliance.

On the federal side, this will need to include clear authorities and dedicated federal oversight. Although the FAA is tasked with creating the guidelines for integrating UAS safely into domestic airspace, the agency is reluctant to deal with issues it considers outside its domain, including security and privacy. While some people have recommended that the Department of Homeland Security (DHS) take on these issues, DHS may be reluctant to take a lead role in what is likely to be a highly complex and contentious issue.

Several witnesses at the July 2013 hearing on "Using Unmanned Aerial Systems in the Homeland: Security Game Changer?" pointed to DHS as best suited to the task.

William R. McDaniel, Chief Deputy, Montgomery County Sheriff's Office, Conroe, TX, points out:

> Now that UAS technology is here, the FAA does not have the experience in its application. The FAA does not have the law enforcement, fire, or emergency management background to be able to relate to the mission of these agencies… we believe they have no real understanding regarding the "critical mission" aspect of UAS operations. If UAS operations remain under the oversight and control of the FAA, as is currently staffers do the case, domestic UAS operations will continue to be severely hampered or limited to the point of being useless.[73]

McDaniel proposes that the DHS Office of State and Local Law Enforcement take the lead, while fellow witness Amie Stepanovich, Association Litigation Counsel for the Electronic Privacy Information Center (EPIC), argued that the DHS Office of Privacy take the lead.

On the other hand, U.S. Representative Michael McCaul (R-TX), Chairman of the House Subcommittee on Oversight, Investigations and Management referenced a GAO recommendation that the Secretary of Homeland Security direct the Transportation Security Administration (TSA) to "examine the security implications of future, nonmilitary UAS operations in the national airspace system and take any actions deemed appropriate.[74]

So where should the responsibility lie? Assuming that DHS should take the lead, several offices will have a stake in the issue, including those noted in the hearing as well as some that have not been mentioned, such as the cybersecurity office. The GAO's recommendation to hand the lead to TSA may have the greatest merit due to the subject; however, TSA may not have the clout needed to gather a coalition of support from across the Department and other interested agencies. Because of the highly political nature of

---

73 Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?: Hearing Before the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, 112th Cong. (2012) (Statement of Chief Deputy William R. McDaniel, Montgomery County Sheriff's Office, Conroe, Texas).

74 Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?: Hearing Before the Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security, 112th Cong. (2012) (Statement of Michael McCaul, Chairman, Subcommittee on Oversight, Investigations, and Management).

this issue, it may be best for a DHS headquarters office such as the Office of Policy to take the lead, with an eventual transition to TSA. Another option would be to give the role to the DHS Office of Infrastructure Protection, which also resides at headquarters and plays an active role in addressing the broad spectrum of threats to the nation's critical infrastructure.

True cybersecurity will require a coalition of the informed and willing, bringing together private developers, customers, trade and industry associations, advocacy groups, and federal, state, local, tribal and territorial partners. Together, this coalition will need to work through the wicked problems stemming securing the cyber front while retaining a transparent, open democracy.

THIS PAGE INTENTIONALLY LEFT BLANK

V. THE LEGAL AND CONCEPTUAL CHALLENGES OF PRIVACY

Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.

—Justice Louis Brandeis, 1891

Americans paradoxically combine an unquenchable curiosity with an insistence on being left alone.

—*Scientific American*, September 5, 2008

Privacy is a nebulous concept has perplexed lawmakers, human rights advocates and commercial enterprises alike. Much like light itself, which is simultaneously a particle and a wave, the notion of privacy can be measured in discrete, measurable units while also existing on a continuous scale where measurement is supremely subjective.

In the U.S., the issue takes on an additional relevance. Founded by pioneers and born out of revolution, the U.S. clings to a strong heritage of individualism that sets it apart from most of its democratic allies. Suspicion of the government is woven into the fabric of the U.S. Constitution, with language that specifically prohibits government intrusion into the life of the individual.

As technology permeates every aspect of modern life, privacy issues provoke debate in professions ranging from advertising to intelligence. Businesses want as much information as they can get on prospective customers, the better to target their services to likely consumers. The government seeks ways to document and track people ranging from entitlement recipients to criminals—whether to improve services and avoid fraud, or to keep a community safe. For the sake of convenience, ordinary citizens willingly leave a trail of their personal activities through commonly used technology ranging from GPS mapping, to online purchases, to value cards.

While each of these activities can seem inconsequential in themselves, questions about privacy hinge on a handful of key issues, starting with how one even defines privacy. In fact, depending on one's perspective, the age of privacy might even be over,

as Facebook founder Mark Zuckerman suggested in 2010,[75] or it may retain such importance that a state or local jurisdiction takes pre-emptive measures to outlaw new technologies like UAS before they have even been introduced locally.

Figure 10 provides a modest demonstration of how technology and privacy laws have evolved together since the American Revolution. While the focus is on the United States, key European Union policies discussed later in this chapter are included for context.

[75] Marshall Kirkpatrick, "Facebook's Zuckerberg Says the Age of Privacy Is Over," *readwrite,* January 9, 2010, http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~ofrKLp0EphACyi

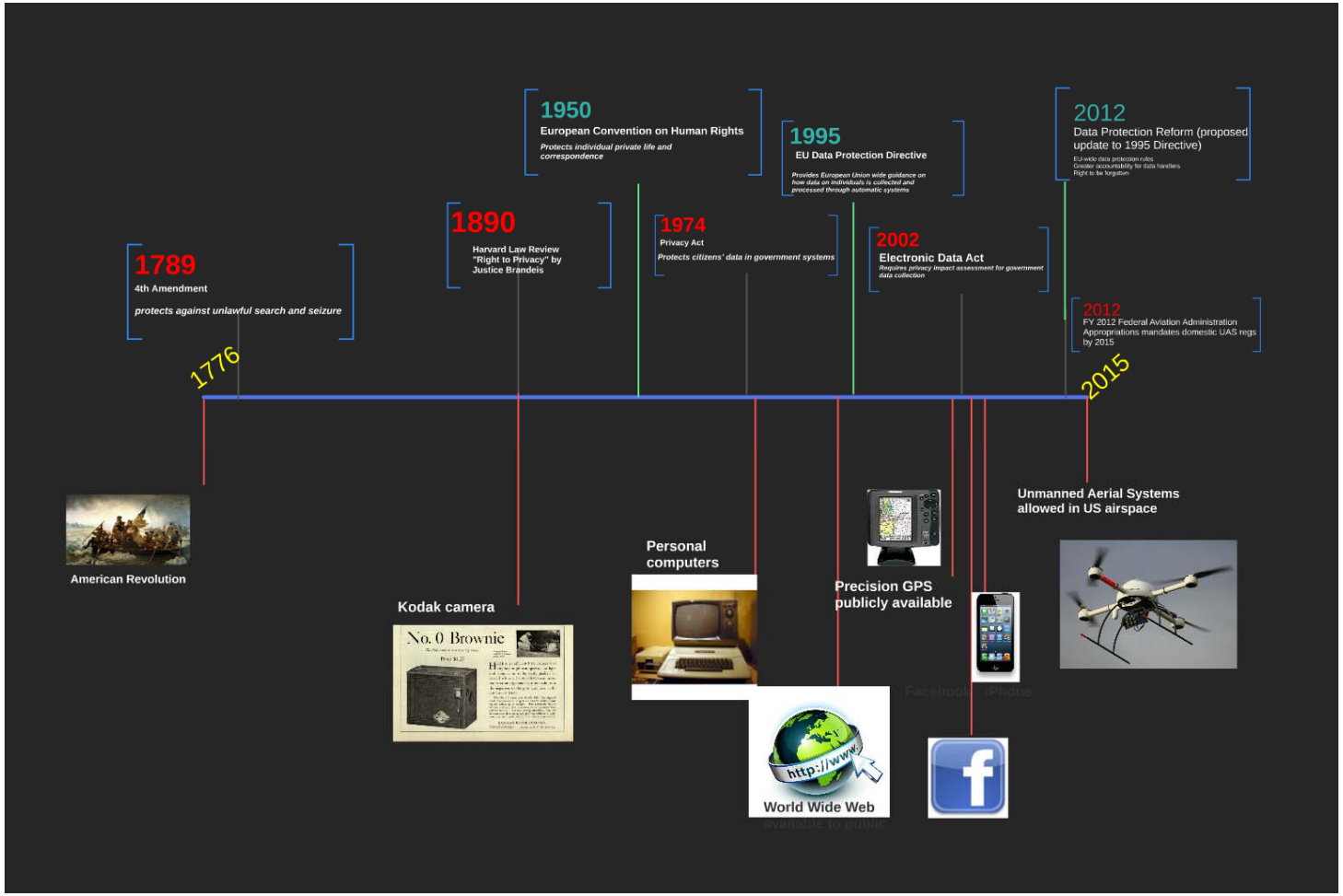


Figure 10. Timeline of Privacy in America[76]

[76] Photos, Prezi.com, accessed January 12, 2014 https://prezi.com/.

In her 2013 thesis, "Minding the Gap: The Growing Divide between Privacy and Surveillance Technology," Debra Kirby provides an in depth examination of the nature of privacy and the laws that impact it, grouping privacy broadly under "conceptual" and "legal" frameworks. As Kirby points out, privacy encompasses intangible concepts, such as cultural and psychological norms. On the other hand, the many attempts to define privacy in a legal context have led to an assortment of incompatible federal and state laws that entwine courts, businesses and citizens in a maze bureaucracy and loopholes.

The U.S. has not yet established a national law governing data collection and privacy, leaving such issues to the nation's 56 states and territories. Some might argue that this is a legitimate free-market approach. Commerce thrives on the ability to target potential consumers with ever increasing accuracy, allowing companies to focus their marketing dollars where they are most likely to reap some benefits.

Apart from Kirby's study, other literature suggests that more tangible issues include who has access to personal data, how it is aggregated and used, how it is transmitted to third parties and ultimately how it is stored or destroyed. Combined, these issues can make it close to impossible to retain anonymity. The "right to be forgotten" or what Justice Brandeis called a "right to have a personality"[77] is rapidly succumbing to a barrage of technological marvels that provide security, comfort and ease. These same technological marvels are increasingly connected and communicating with each other in the Internet of things that spans the globe, allowing the humans that they serve to relinquish more and more control over routine tasks like monitoring supplies or maintaining a safe distance from the car ahead.

Even as regulators and policy makers scramble to catch up with technology introduced in just the past few years, dramatic new advances are carrying society forward in a technological tidal wave. As government bureaucracies at all levels struggle to keep pace with technological developments, they fall further behind the curve. Yet, in many respects, the increasing intrusion into personal lives is nothing more than an aggravation

[77] Louis D. Brandeis, and Samuel D. Warren, *The Right to Privacy* (Cambridge, MA: Harvard Law Review, 1890), E-book, http://www.gutenberg.org/files/37368/37368-h/37368-h.htm.

that is part and parcel of a global trend toward increased transparency in all areas of life and government. In this interconnected, programmable world, the domestic UAS may emerge as a potential lightning rod for the debate over privacy.

A. THE EU AND UK APPROACH

Since there is no direct precedent for widespread commercial and domestic government UAS use, an analogy might be found in how the European Union (EU)—and the United Kingdom in particular—has addressed privacy issues related to pervasive use of closed circuit television (CCTV) to monitor public safety and security issues. The EU and its member countries provide a good sounding board for how such issues might be handled in the United States, which was largely a derivative of European law and culture when the nation was established. As a conglomerate of self-governing democratic nations, the EU as a structure loosely resembles the U.S. structure as a single entity comprised of many self-governing states and territories, with tens of thousands of semi-independent local jurisdictions. Although the EU is not a federation like the U.S., it does provide overarching laws that supersede national legislation in some areas of policy.

A key difference between the two regions is that European nations have dealt directly with terrorism on national soil for far longer than has the U.S., allowing European populations more time to adjust to a level of government surveillance that Americans might find intrusive. A factor that could complicate direct comparisons in approaches to privacy is that the U.S. has a fundamental distrust of federal government, an attitude born out of revolt against heavy handed colonial rule and safeguards written into its constitution. For the most part, EU member countries seem to have transitioned more gently away from authoritarian monarchies to shared power with voters (with key exceptions like France, which experienced a violent revolution inspired by America's successful bid for freedom).

Landmark doctrine includes the 1950 Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms, specifically Article 8 on the right to respect for private and family life. Other foundational legal guidelines include the United Kingdom's *Data Protection Act of 1995* and the related *Directive 95/46/EC of the*

European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Guidelines for CCTV use have been developed out of these earlier efforts to deal with the growth of electronic data related to individuals since the Internet was introduced to the public.

1. Privacy, Transparency and Surveillance

> *Secrecy is to government what privacy is to persons. They both rise or fall —at present they're falling—on the same technological changes and on the same cultural proclivities for modesty on the one hand or exhibitionism on the other.*
>
> —Joel Brenner, former National Security Agency senior counsel

One of the primary complaints by opponents of UAS is fear that the government will be conducting surveillance on Americans. In his book *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage*, Joel Brenner claims that "this isn't a case of heavy-handed government surveillance. It's a case of pervasive, light-handed surveillance by just about everybody, producing massive amounts of information that can be correlated with a few keystrokes or mouse clicks. Transparency has come to the intelligence business."[78] Moreover, intelligence is not limited to government; in fact, businesses may be the largest consumer of intelligence when it comes to knowing about their customers and competition.

In 2006, the UK-based Surveillance Studies Network submitted "A Report on the Surveillance Society: For the Information Commissioner." In contrast to the American Civil Liberties Union (ACLU), which hopes to prevent a surveillance society,[79] the UK report begins by stating that "It is pointless to talk about surveillance society in the future

[78] Brenner, *America the Vulnerable*, 163.

[79] Crump, "Protecting Privacy from Aerial Surveillance," 1, 11–12.

tense. In all the rich countries of the world everyday life is suffused with surveillance encounters, not merely from dawn to dusk but 24/7."[80]

Rather than expend effort attempting to retroactively address this state of surveillance, the report suggest that "we shift from self-protection of privacy to the accountability of data-handlers."[81] This pragmatic approach assumes that cultural norms are evolving toward transparency in all areas, as Zuckerman and Brenner claimed.

The report notes that "technologies are at their most important when they become ubiquitous, taken for granted, and largely invisible."[82] If one accepts this position, then being "largely invisible" might also include the confidence derived from the knowledge that personal data that is well-protected against abuse and misuse.

To address concerns in this area, the UK established the Information Commissioner's Office as "The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals." The larger EU community has also adopted clear guidelines, including the European Convention on Human Rights, and the European Union Data Retention Directive. In contrast, the U.S. has no similar structure or national guidelines, instead relying on a network of agency-based privacy offices, various laws that address aspects of the privacy issue, and corporate self-regulation, consistent with a *laissez-faire* tradition.

B. TOWARD A POLICY OPTION TO PROTECT PRIVACY WHILE MAINTAINING TRANSPARENCY

Over the past several decades the EU had enacted or proposed a number of laws to protect privacy in an age of increasingly sophisticated technology and global interconnectedness. Key policies are summarized in the following pages.

---

[80] Kirstie Ball et al., *A Report on the Surveillance Society: For the Information Commissioner*, UK: Surveillance Society Networks, 2006, 1.

[81] Ball, *A Report on the Surveillance* , 6.

[82].Ibid., 10.

1. European Convention on Human Rights

Article 8 of the European Convention on Human Rights is frequently cited to emphasize the fundamental human right to privacy. Indeed, the first part of Article 8 seems clear on this point, stating: "Everyone has the right to respect for his private and family life, his home and his correspondence."

However, the full explanation provides significant latitude for domestic surveillance, stating:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[83]

Within the full scope of Article 8, it is entirely conceivable that UAS could be used for public good, such as law enforcement or monitoring everything from critical infrastructure to agriculture to environmental issues. In short, UAS could be used for anything requiring an aerial picture of facilities, property or constituencies, especially where such monitoring falls into the "dull, dirty or dangerous" category, in which a human operator might be at risk. However, such latitude also requires considerable judgment on the part of those conducting this surveillance, as well as strong trust building efforts with stakeholders to ensure that the spirit of Article 8 is preserved.

2. EU Directive 95

EU Directive 95 establishes a consistent approach to data privacy for all EU member countries, primarily to promote the free flow of commerce where otherwise differing privacy laws might create obstructions. There is, however, a clear exception to the right to privacy where sound and images are recorded, "such as in cases of video surveillance…if it is carried out for the purposes of public security, defence (sic),

[83] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14. Rome, 4.XI.1950. http://conventions.coe.int/treaty/en/treaties/html/005.htm. Accessed March 5, 2014.

national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law."[84]

As Kirby noted, a key difference between the U.S. and the EU— and in particular, the U.K.—is that there is no single agency in the U.S. with the sole responsibility for overseeing privacy laws and developing codes of practice. In fact, in this area, the U.S. might be considered a bit of the Wild West, with few sheriffs and little protection from commercial interests that aggregate and sell personal information to third parties.

3. Safe Harbor

The Safe Harbor initiative was established in 2000 to provide U.S. companies with guidelines for handling personal data when conducting transactions with EU member nations, and to assure EU members of a minimum standard of security. While it is largely incumbent on the private sector participants to monitor and self-certify themselves, if they do breach the rules there are financial penalties as well as the threat of being excluded from the Safe Harbor initiative.

4. 2012 Data Protection Reform

In July 2012, the European Commission suggested the following key updates to the landmark 1995 Data Protection Directive[85]:

- A single set of data protection rules valid across the EU, enforced by stronger national authorities, enabling companies and individuals to work with their own national representative, regardless of where in the EU the data issue might originate.
- Increased responsibility and accountability for those processing personal data.
- A 'right to be forgotten' to help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.

---

[84] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[85] "Why Do We Need an EU Data Protection Reform?" European Commission, accessed August 16, 2013, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

C. ADVOCACY ORGANIZATIONS

A number of organizations have provided suggested guidelines on protecting privacy as technology fosters increasingly high fidelity composites of individual lives. Among the organizations at the fore of the issue are Privacy International, a UK-based charity founded in 1990 and, in the U.S., the Electronic Privacy Information Center (EPIC), based in Washington, DC. These and other advocacy organizations are watching with concern as private sector-driven technology converges with the introduction of UAS into domestic airspace.

Although EU Directive 95 is primarily directed at business use of personal data, in July 2013, Privacy International introduced its own version focusing on government use: the "International Principles on the Application of Human Rights to Communication.[86] These 13 principles cover everything from legitimacy of the surveillance effort to proportionality of surveillance benefits over user rights to safeguards against illegitimate access. This last piece is especially important in light of very weak cybersecurity safeguards commonly used by the private sector.

D. RECOMMENDATIONS FOR APPLYING EU AND UK GOOD PRACTICES IN THE U.S.

Technology will continue to outpace privacy law, however, the EU and UK might offer a number of good lessons that could be applied in the U.S.

Often developed with the consumer in mind, many EU guidelines strive to protect privacy in a global economy that relies heavily on the collection and transfer of data on individuals. At the same time, these laws also tend to provide wide latitude to government entities conducting surveillance and data collection in the interest of public safety, national security and similar public services.

Of the various measures already put in place in the EU, the move toward greater accountability for those who are collecting data seems most likely to establish protections

[86] Carlie Nyst, "Introducing the International Principles on the Application of Human Rights to Communications Surveillance," July 31, 2013. The Privacy International Blog. https://www.privacyinternational.org/blog/introducing-the-international-principles-on-the-application-of-human-rights-to-communications.

where they can be enforced. However, to adopt this as a primary approach in the U.S., it would also require a concerted effort to engage privacy groups and the general public. This effort should be supported by a transparent government approach, including well publicized opportunities for public comment supported by an outreach and education campaign conducted by a partnership of government agencies, media partners and advocacy organizations.

Other key components of EU laws include establishing a single national office to provide oversight and streamline coordination on privacy issues, as well as exemptions for critical life safety and protection of property issues, such as national or economic security.

Of interest, advocacy groups like EPIC and the Electronic Frontier Foundation (EFF) also favor a national guideline, rather than a state-by-state approach, stating, "National governments must put legal checks in place to prevent abuse of state powers, and international bodies need to consider how a changing technological environment shapes security agencies' best practices."[87]

[87] "Privacy," Electronic Frontier Foundation, accessed August 20, 2013, https://www.eff.org/issues/privacy.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FUTURE CONSIDERATIONS, ANALYSIS AND RECOMMENDATIONS

For those who have been following the UAS integration debate, 2015 looms like an event horizon, after which there is no turning back. Capable of carrying a wide variety of sensors, from highly sensitive cameras to thermal imaging equipment, UAS also offer flexibility of design and size limited only by imagination and the laws of physics.

To some, this heralds the dawn of a new age in commercial enterprise and innovation that spans everything from emergency response to agriculture to environmental protection. However, without adequate privacy rules in place, others worry that 2015 will mark the end of privacy, as they envision tens of thousands of prying eyes in the sky.

This final chapter will make an attempt to peer into the future, using several plausible scenarios to illustrate possible alternate futures based on current trends and technology, followed by a final analysis and recommendations.

A. FUTURE SCENARIOS 2050

This thesis presents an array of issues within the context of UAS and the national airspace. These included conceptual and tangible items, such as the increasingly rapid evolution of technology, the Internet of Things, autonomy, public opinion and cybersecurity. Drawing from these and other current phenomena, four potential future scenarios are explored briefly below.

1. On the Sidelines

Due to concerns over massive intelligence leaks by Edward Snowden and bad press stemming from U.S. military drone strikes overseas, the American public effectively halts plans to allow UAS into national airspace. Meanwhile, China, India, Israel, Australia, Japan, Canada and a host of other countries develop a multi-billion dollar global UAS industry. Drawn by the economic potential of overseas opportunities, Boeing all but stops investing in research and development on airplanes and focused its

efforts on the lucrative international UAS market. A diverse assortment of corporations that rely on air transport, such as UPS and other air cargo companies, are likewise finding more lucrative markets abroad, where they can take advantage of lower cost UAS. John Deere has set up an air division in Canada to sell agricultural UAS such as cropdusters, and many Hollywood cinemaphotography companies have relocated their operations to Bollywood. As a result of this cumulative exodus of investment and innovation, the U.S. loses its edge as a global economic force, and many wealthier families start sending their children overseas for their education, in hopes of better opportunities abroad.

2. Government Leads the Way

Disregarding the unease expressed by many Americans over news about government surveillance and military drone attacks overseas, the federal government focuses efforts on dealing with safety issues related to UAS integration and moves quickly to open up national airspace. Lacking balanced media coverage and clear information on how law enforcement, DHS and other agencies are collecting information, rumors spring up to fill in the gaps and spread like wildfire. The media feeds off rumors that the government is spying on its own population, seeking out "experts" to share their opinions on Fox News and other media outlets. Perception becomes reality, and people become increasingly frustrated and concerned. Finally, the government responds with an information campaign, but it is too late. The opportunity is lost and the public does not trust official sources. Extreme right wing groups and extreme left wing groups find common ground in their dismay over what they perceive to be an Orwellian trend. Opposition gathers momentum, and other issues like federal entitlement programs and taxes are thrown into the mix, fueling anger. Ultimately, a gaping divide opens between the government and its people.

3. The Private Sector Leads the Way

Stimulated by a heady mix of unlimited business opportunities and few regulations, large and small businesses and entrepreneurs vie for a place in the new economy. Feeding off of each other's ideas, UAS applications evolve quickly. Now people in isolated communities can receive rapid medical support. Lost hikers and

Alzheimer's patients can be quickly located and brought to safety—as can criminals. Budget-conscious communities can expand their emergency services capabilities with unmanned law enforcement, police and fire aircraft. New job markets open up to support ever more ingenious UAS applications. However, in the rush to break open new territory, massive amounts of data collected by UAS sensors are exposed through cybersecurity vulnerabilities, and more and more people find their most intimate moments interrupted by a new breed of paparazzi that pursues the ordinary citizen for reality web shows. As UAS are linked into the Internet of Things, hackers find ways to divert UAS by smart phones. With no clear line of accountability, personal data succumbs to the Tragedy of the Commons, and privacy ceases to exist.

4. A Coalition Forges a Balanced Path Forward

Anticipating unlimited opportunities, but conscious of potential pitfalls, a coalition of government, corporate and advocacy leaders comes together to hash out a vision for how to leverage the benefits of UAS while maintaining security and privacy. Together, this group provides checks and balances to varying approaches and comes to a consensus that the goal of any policy should be that UAS technology works in support of the American people. The coalition develops clear guidance and accountability for privacy and security issues, while promoting a competitive environment that invites innovation. With this strong foundation, and supported by an aggressive outreach and education campaign, the American public feels more confident in the opportunities that await. Soon, UAS are as common and utilitarian as household appliances, bringing all of the benefits of a corporate-led integration along with the safety net of strong cybersecurity and privacy protections.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ANALYSIS

Introducing UAS into domestic airspace by 2015 is an ambitious plan, highly spiced with a peculiar mix of American individualism, massive defense industrial base money, politics, civil liberties interests, and intellectual curiosity. Developing a policy that achieves the intent of Congress' mandate while retaining the less tangible and sometimes competing American values, like transparency and privacy, will require the active participation of a broad, bipartisan coalition of unlikely partners.

The key issues discussed throughout this thesis are tightly interdependent, and should be addressed comprehensively. Privacy and economic interests depend on rigorous cybersecurity. Laws governing these issues not only must keep pace with technological advances, but must also peer into the future and address the unanticipated consequences. Policy must be developed through a transparent, public process, in which the media, advocacy groups, Congress, industry, academia, emergency responders and all of the other stakeholders are heard and their concerns considered.

A successful policy can contribute to a new era in flight technology. Because of the extremely high degree of design flexibility, UAS could eventually support almost any type of airborne effort, from crop and pipeline monitoring to journalism to lower cost cargo transportation and mass medical support. An effective policy would also reflect a common vision of where the country wants to be, in terms of balancing individual liberties with economic benefits of developing a new domestic industry. In such a scenario the nation would fully harness technology to work "for" the population, and not against it.

Lacking a strongly knit, well considered policy in the near future, an extreme "worst case" scenario could be a dystopian surveillance society in which privacy—and America as we know it—ceases to exist. Likewise, if we do not move forward quickly with UAS integration, we will lose any chance of global industry leadership in a nonlethal UAS (i.e., nonmilitarized) market, as other countries like Japan and Canada move forward. Another risk of ineffective policy is a bureaucratic maze of conflicting

laws at the federal, state and local levels, which make it impossible to leverage UAS technology or to become competitive in the budding domestic and global industry.

A. COSTS

Should the U.S. fail to move forward with integrating UAS domestically, the potential economic costs of lost business could be in the billions or tens of billions of dollars.

However, the cost of developing and implementing a policy, in terms of tax payer dollars, should be relatively low. Costs to develop policy may be counted in terms of staff hours for government workers, and minimal costs to establish a menu of stakeholder engagement options, such as online and in person forums, as well as some travel costs for the program managers to visit different testing sites.

At a state and local level, costs would include training for UAS pilots, especially in the first responder community. These costs are still less than the cost of training fixed and rotary wing pilots and buying equipment for manned aircraft, so there is a cost savings. To offset these and other costs, state governments might decide to offer tax incentives to promising UAS developers to base their operations in state. The indirect costs in tax dollars would be offset by jobs gained and tax revenues from the eventual sale of the unmanned systems.

B. COURSES OF ACTION

There really is no “status quo” on this emerging issue. However, if one were to point to something resembling status quo, it might be current military use of armed drones and unarmed surveillance UAS. Other options might include an aggressive plunge forward to meet congressional deadlines, or a negotiated integration in which UAS are integrated in phases, over a span of years.

1. Maintain Status Quo

To maintain status quo, the U.S. would keep its airspace closed to UAS and leave such use entirely to the military. The benefits of this course of action might include more

dedicated funding to military UAS research and development and avoiding disruption of domestic civil society as the public adapts to UAS at home. However, in this budget climate it seems unlikely that additional government funds would be available. It is also difficult at best to ignore a congressional mandate to open U.S. airspace. Furthermore, to ignore the potential for domestic use would put the U.S at a significant competitive disadvantage, as a wide array of allied nations and a number of nonallied nations are actively exploring or even using UAS at home.[88]

2. Plunge Ahead

An alternate course of action would be to adhere strictly to the word of the congressional guidance to open up airspace by 2015, and allow broad and immediate use of UAS. While this could offer immensely exciting opportunities to stakeholders ranging from law enforcement to private corporations, there is a significant potential downside of implementing this new technology without a supportive infrastructure of carefully considered guidance and matching air traffic control technology. All of the current issues- privacy, civil liberties and safety—would be compounded by bad publicity and lawsuits that would inevitably arise as UAS (especially smaller ones that would be more accessible to individual citizens) are put in the hands of untrained federal, state and local agencies or civilians. Bad press could work against the UAS industry, slowing down adaptation or even killing the effort altogether if there is enough public and congressional pushback, as in the case of the now-defunct DHS Office of Intelligence and Analysis National Applications Office.[89]

3. Phased Integration

A third course of action would be phased integration over a span of several years. The FAA could focus its initial guidance on UAS use for public safety efforts like firefighting and meteorological monitoring, then expand quickly to law enforcement and

---

[88] U.S. Air Force, *United States Air Force Unmanned,* 3.

[89] DHS I&A attempted to take a cost-saving approach to developing a Department-wide UAS capability. However, the public quickly shut this effort down, over fears that it would lead to illegal surveillance on American citizens. Instead, UAS have been piloted successfully by DHS components, like CBP and on an extremely limited basis, by FEMA through agreements with other agencies.

homeland security agencies support public safety and disaster response. (A 2003 public opinion survey by the American Institute of Aeronautics and Astronautics found that the general population would accept commercial and humanitarian use of UAS.[90]

4. A Role for Standards

In a related effort, standards organizations like the ANSI Homeland Security Standards Panel should develop consistent guidelines that will support interoperability of various UAS communications systems, as well as the adoption of UAS in a safe and publicly acceptable manner. Interoperable communications will increase safety efforts by enabling manned flights to communicate with UAS operators. It would also significantly increase joint law enforcement and homeland security efforts, allowing greater real-time information sharing, as encouraged in numerous strategies, including Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.

While these two efforts are working on guidance, the public will become accustomed to low-altitude "toy" UAS such as Verizon's "Parrot" quadcopter that can be controlled through a mobile device. From such commercially use, it is a relatively small step for public acceptance of much broader market uses. An optimal situation would one in which a market demand is created for UAS, whether in government or public use. A strong marketing campaign that publicizes success stories would greatly increase this pull.

Homeland security and law enforcement agencies have already started working toward UAS integration either in pilot projects or through research and training. Moreover, government officials are not driven by market decisions and are more risk averse, thus increasing the likelihood of successful integration. Open market use can be phased in at a slower rate, based on lessons learned through the government use, and a corresponding publicity campaign demonstrating the benefits of public use. Policy makers should also review the suggested guidance already developed by the lead industry and public advocacy voices on this issue, including the American Civil Liberties Union

[90] Darnell, "Unmanned Aircraft Systems," 52.

(ACLU), the Human Rights Watch and The Association for Unmanned Vehicle Systems International (AUVSI).

The UAS industry is poised to drive the U.S. into a new era of public and private aviation. Usage has the potential to span just about every aspect of domestic society. With a practical, common sense approach, the public and private sectors can work together to make UAS a widely used and appreciated tool, as well as an economic advantage.

C. POLICY RECOMMENDATIONS

The U.S. has a complex relationship with the issue of privacy. Given the privacy concerns being raised over the integration of UAS into domestic airspace, the federal government should be proactive in establishing clear guidelines. One way to do this is to look to allies that have already accumulated experience with similar issues and adopt promising practices, such as those listed earlier. A final consideration is that U.S. business interests may lobby hard against new regulations of any sort, so an alternate approach would be to expand the Safe Harbor Initiative nationwide, as a way to phase in stronger privacy legislation later.

The following policy recommendations expanding on the principles of "safety, professionalism and respect" espoused by AUVSI, and synthesize recommendations from civil liberties advocates, international good practices and common marketing principles,[91] as well as some of the author's own thoughts.

1. Establish Boundaries

There is discussion in the online community revolving around "not over my back yard" opposition to UAS. Steps that could ease these concerns might include:

- Establish "no fly" zones around communities, with exceptions for law enforcement, emergency services and licensed carriers (e.g., cargo transport)

[91] The reference to marketing principles is based on the author's own background and work experience.

- Develop UAS “airways” (similar to current roadmaps and highways for land and channel markers for maritime traffic) so the majority of UAS traffic flows along established routes
- Expand personal property boundaries vertically, to cover the airspace over homes, up to 400 feet (the current standard for small UAS like quadcopters)

2. Accountability through Identification

Every person who drives a motorized vehicle is required to be qualified and accountable. Typically, this is through licensing and training. Drawing on current practice for land-based vehicles, the following practices could alleviate privacy concerns by increasing accountability:

- Establish a UAS version of the Department of Motor Vehicles, with mandates similar to car drivers: licenses, registration, license plate- all to create accountability
- Clearly mark police and emergency services UAS, similar to vehicle markings

3. Engage Stakeholders

Messaging used in outreach by policy makers, industry and the media should make every effort to frame the coverage of UAS in a way that brings humanity back into the picture and reaffirms that technology works for the American public, never against. Currently, a handful of police departments around the country are attempting to expand their capability with UAS. However, community backlash has threatened to shut down some of these operations before they have taken flight. Some communities, like Charlottesville, VA, prohibited UAS before the local law enforcement even considered their use. Early, continual stakeholder engagement is key to the success of controversial efforts like the use of UAS. Some recommendations include:

- Work closely with the ACLU and other opponents to develop common-sense guidelines
- Let communities vote on whether they want local law enforcement to use UAS, and to what extent
- Let the market drive demand. Rather than government driving usage, let commercial interests drive demand for UAS by demonstrating value (e.g., cargo transport, commercial and private security, etc.)

- Conduct a public outreach campaign to test public opinion and introduce the concept of UAS and the benefits they can bring
- Demystify UAS with "show and tell" events, similar to what emergency services do already; allow people to touch and see UAS, and perhaps even publicly demo them in a controlled environment

4. Employ only NonLethal Payloads in National Airspace

Fully autonomous UAS are already in development. To avoid a highly undesirable direction in the future, UAS used for routine homeland security or law enforcement activities should not carry lethal payloads in domestic airspace.

5. Adapt Current Surveillance Laws to Unmanned Aircraft

Government entities should adhere to current laws related to warrants, wiretaps and other surveillance guidance, as well as current guidance related to law enforcement use of airplanes and helicopters.

6. Develop a Single, National Privacy Standard

Airspace rules transcend boundaries, in keeping with the nature of the airspace itself. Likewise, privacy laws applied to UAS should be consistent nationwide to allow for free flow of commerce and homeland security coordination among federal, state and local entities. This law would govern the legitimate collection, aggregation and disposal of personal data through aerial surveillance, whether for commercial or government purposes.

7. Establish a Federal Office in Charge of Monitoring Data Privacy, with State-Based Field Offices

At present, no single office is in charge of privacy, making oversight more complex than necessary. A single, national office will reduce bureaucracy and streamline processes related to collecting, aggregating and disposing of data. It would also provide citizens with a single point of contact for accessing, correcting or petitioning for disposal of personal data.

8. Enforce Accountability of Data Collectors

Making the data collectors accountable for the integrity, security and proper disposal of data collected by UAS is the most effective way to ensure that data will be handled appropriately. UAS operators will be responsible for ensuring that streaming images and sound is protected against illegal access by encryption or other means.

9. Provide Limited Exemptions for Activities Conducted in the Interest of National Security, Life Safety, and Protection of Property

These are the most consistent exceptions found in the EU and UK laws, and should apply equally in the U.S. However, such exceptions should be made judiciously and in keeping with existing U.S. laws government warrants, search and seizure and other civil rights.

10. Manage Risk and Enforce Cybersecurity from the Inside Out

Cybersecurity is still on the periphery of most people's awareness. Yet, as Brenner writes, leaders must "accept that their information systems are compromised and must plan accordingly."[92] Risk and responsibility for risk must be assigned definitively for each step along the UAS supply chain, from designer to end user. Brenner advises companies to control what and who is on their systems, protect information of value, patch networks, train staff, audit and manage overseas travel behavior.[93] In the case of UAS, this could mean tighter controls over the manufacturing process, enhanced security screening for employees with access to any part of the research, development and manufacturing process, stricter enforcement of basic computer hygiene by all company employees, and better funding and increased authority for the department responsible for corporate security.

D. MEASURING SUCCESS

If media can be assumed to reflect the voice of the concerned—through its traditional role of encouraging transparency and public debate—then one measure of

---

[92] Brenner, *America the Vulnerable,* 91.

[93] Ibid., 222–224.

success would be positive or neutral media coverage of UAS, including a growing differentiation between armed military drones and the types of UAS more likely to be used commonly in the U.S.

Another indicator of success could be measured in the quality and quantity of stakeholder feedback collected from representative segments of all major impacted groups (i.e., intergovernmental partners, first responders, general public, civil liberties groups, business and industry) as policies are developed. Stakeholders should continue to be engaged as policies are implemented.

A long term measurement could start with the rollout of a national policy governing domestic UAS. Positive or neutral media coverage would continue to be a good measure, as would minimal stakeholder backlash. The latter would indicate that policy makers had effectively addressed key stakeholder concerns and maintained an active public engagement campaign throughout the process to ensure transparency. Public opinion polls could capture a more scientifically accurate measure of acceptance of domestic UAS.

Ultimately, an effective policy would support U.S. industry and facilitate a move to global leadership in production of domestic/nonmilitary UAS, while UAS technology enhances the quality of life in the U.S.

E. CONCLUSION

As we stand on the precipice of a new era, we still have choices. Will the U.S. take a step back, preserving what it knows and withdrawing from a global technology revolution? Or will we take a leap of faith, spreading our wings and soaring into the unknown?

What do we stand to lose? If we opt to maintain status quo—in other words, an America where UAS are not part of the common experience—then the American economy could lose its opportunity to leverage an emerging, multibillion dollar global industry. The nation could also lose the opportunity to leverage this technology to improve lives.

For pessimists, a worst case scenario might be one in which government entities use UAS for pervasive, persistent mass surveillance, monitoring everyone, all the time. In such a scenario, privacy would become meaningless. Fully autonomous—and eventually, perhaps even self-aware—UAS would be linked into the Internet of Things, able to connect with your credit cards, smart phones, bank account, car, iPad—anything with a digital signal—tracking individuals regardless of their criminal intent and generally stifling free expression.

In an optimal scenario, the country would benefit from UAS that bring medical treatment to people who live in remote locations or fly in swarms to provide mass vaccinations during pandemics. They would monitor thousands of miles of pipelines and provide temporary communications support after disasters. Lost hikers or escaped convicts could be found quickly and chemical hazards could be monitored with greater transparency and attribution. At the same time, people would know that any data collected is handled, stored and disposed of securely, and that an individual may access and correct information on themselves with minimal bureaucracy.

F. RECOMMENDATIONS FOR FUTURE RESEARCH

Swirling around in the not-too-distant future are the progeny of today's ideas—autonomy, self-aware robotics, 3-D printing, organic machinery….all of these and more will influence the future of UAS. This thesis merely scratched the surface of the most immediate issues facing the nation as UAS are introduced into national airspace. The implication of other technology under development and their convergence with UAS opens up virtually unlimited areas of exploration.

What will happen when autonomous UAS become self-aware? Could they diagnose and repair their own mechanical failures, thus improving safety? How might 3-D printing challenge efforts to institute accountability, or the ability of law enforcement to track anonymous and illegitimate UAS? The cyber security aspects alone could comprise the sole focus of another thesis.

We are Da Vinci's children. We are creating the machinery and the ideas that can launch us into destruction or Renaissance. As such, we face challenges similar to those of

the great engineer/inventor/artist Leonardo da Vinci, many of whose ideas for disruptive innovations were hundreds of years ahead of their time.

Whether one believes that today's population is better prepared to adapt, having been primed by a world that is already technologically advanced, or that technology is advancing too fast to keep up, the policies we put in place and decisions taken today will have impacts far into the future. There is still time to get it right, but the window is closing fast.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. USEFUL LINKS

- Certificate of Waiver and Authorization Online Resources: http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/
- FAA Frequently Asked Questions about UAS: http://www.faa.gov/about/initiatives/uas/uas_faq/
- Federal Aviation Administration Aerospace Forecast Fiscal Years 2013–2033: http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2013–2033/media/Unmanned_Aircraft_Systems.pdf
- Congressional Unmanned Systems Caucus: http://unmannedsystemscaucus.mckeon.house.gov/
- Association of Unmanned Vehicle Systems International: http://www.auvsi.org/AUVSI/Home

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. COMPARISON OF KEY PRIVACY RULES IN U.S., EU

Law or Regulation	Right to Privacy	Exceptions	Notes
Fourth Amendment (1789)	Protects individuals • Persons • Houses • Papers • Effects	Probable cause Warrant	Part of the Bill of Rights; enacted in response to treatment by British soldiers during the Revolution Does not address electronic privacy
Privacy Act of 1974	Protect U.S. citizens and legal alien residents Specifically addresses the protection of personal data in government systems Broadly inclusive of any "item, collection, or grouping of information about an individual that is maintained by an agency" Allows individuals to request a	• Security of the President • Government contractors • Criminal law enforcement • Central Intelligence Agency	

Law or Regulation	Right to Privacy	Exceptions	Notes
	correction of their personal data		
Sec. 208, E-Government Act of 2002	Requires government entities to conduct a privacy impact assessment before employing technology to collect databases of personally identifiable information Government must provide information on • what information is to be collected • why the information is being collected • intended use • who will have access • what notice or opportunities for consent would be provided to individuals regarding what information is collected and how • how the information will be secured; • whether a system of records is being created under section 552a of	• Sensitive information may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.[94]	Created as part of an overarching act to move the federal government toward electronic-based (web-based) citizen services

[94] Electronic Privacy Act of 2002, Sec. 208.

Law or Regulation	Right to Privacy	Exceptions	Notes
	title 5, United States Code, (commonly referred to as the ‘‘Privacy Act’’)		
European Convention on Human Rights (Article 8) (1950)	Protects individuals • private and family life home • correspondence	“in accordance with the law and (as) necessary in a democratic society” • national security • public safety • economic well-being of the country • prevention of disorder or crime • protection of health or morals • protection of the rights and freedoms of others	Enacted post WWII, prior to the public introduction of the Internet
EU Data Protection Directive (Directive 95) (1995)	Provides EU-wide guidance on how data on individual is collected and processed through automatic systems • developed to protect individuals in new age of automated data collection • promotes commerce across national boundaries	Recording sound and images, “such as in cases of video surveillance” when carried out for • national security • defence (sic) • public security • preventing, investigating, prosecuting crime or of breaches of ethics for regulated professions • important economic or financial interest of a Member State or of the	Developed when the Internet was new to the public Primary focus areas: ensure functioning market and individual data protection

Law or Regulation	Right to Privacy	Exceptions	Notes
		European Union, including monetary, budgetary and taxation matters	
UK Data Protection Act (1998)	Developed to bring the UK into compliance with EU Directive 95; Ensures that data collected by businesses, government and organizations is: • used fairly and lawfully • used for limited, specifically stated purposes • used in a way that is adequate, relevant and not excessive • accurate • kept for no longer than is absolutely necessary • handled according to people's data protection rights • kept safe and secure • not transferred outside the UK without adequate protection[95]	Extensive exemptions include, but are not limited to: • national security and the armed forces • crime and taxation • regulatory activity	The list of exemptions is exhaustive, and covers all aspects of life. Of note, key criteria include intended use.
Safe Harbor Initiative (2000)	Agreement between the U.S. and the EU to address discrepancies in	No exemptions	

95 "The Data Protection Act," GOV.UK, accessed August 20, 2013, https://www.gov.uk/data-protection/the-data-protection-act.

Law or Regulation	Right to Privacy	Exceptions	Notes
	privacy protections • Provides U.S. companies with guidance to meet EU privacy standards • U.S. companies self-certify (built on trust)		
EU Data Protection Reform (proposed update to Directive 95) (2012)	Balances interests of commerce and individual privacy • Single set of data protection rules for EU countries • Companies can work with single national data protection authority—in the EU country where they have their main establishment • Accountability of data processors • National data protection authorities will be strengthened so countries can better enforce EU rules at home • The 'right to be forgotten' to manage data-protection risks online.	No new exemptions noted	• Addresses the variation in how EU member countries interpret and apply Directive 95 • Addresses rapid technological changes, including social networking, cloud computing, and the digital trail that individuals leave through daily use of technology
Privacy International's 13 Principles (proposed 2013)	• Legality • Legitimacy • Necessity • Adequacy • Proportionality	Exceptions must be based in law	Privacy International is included here as representative of the dissenting

Law or Regulation	Right to Privacy	Exceptions	Notes
	• Competent judicial authority • Due process • User notification Transparency • Public oversight • Integrity of communications and systems • Safeguards for international cooperation (apply the higher level of protection for users) • Safeguards against illegitimate access		opinion from government on issues of privacy. Of note, their 2007 world map of "surveillance societies" places the U.S., the UK and most of the first and second world countries in the category of endemic surveillance societies to "weak protections"[96]

96 "Map of Surveillance Societies around the World," Privacy International, accessed August 20, 2013. https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/phrcomp_sort_0.pdf.

LIST OF REFERENCES

Air Line Pilots Association. *Unmanned Aircraft Systems: Challenges for Operating Safely in the National Airspace System*. White paper. Washington, DC: Air Line Pilots Association, 2012.

Associated Press. "FAA Announces Drone Testing in Six States." December 30, 2013.

Association for Unmanned Vehicle Systems International. "Unmanned Aircraft System Operations Industry 'Code of Conduct.'" Accessed February 2, 2013 http://www.auvsi.org/conduct.

Aviation Pros. "Industry Releases 'Code of Conduct' for Unmanned Systems Aircraft Operations." Accessed February 2, 2013. http://www.aviationpros.com/company/10611151/the-association-for-unmanned-vehicle-systems-international-auvsi.

Ball, Kristie, David Lyon, David Murakami Wood, Clive Norris, and Charles Rabb. *A Report on the Surveillance Society: For the Information Commissioner*. UK, Surveillance Studies Network, 2006.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York: Penguin Press, 2011.

Christensen, Clayton. *The Innovator's Dilemma*. New York: HarperBusiness, 2000.

Committee on Homeland Security, Chairman Peter T. King's Office, "Statement of Chairman Michael McCaul (R-TX) Subcommittee on Oversight, Investigations, and Management, Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?" News release, July 19, 2012. http://homeland.house.gov/sites/homeland.house.gov/files/07-19-12%20McCaul%20Open.pdf.

Crump, Jay Stanley, and Catherine Crump. *Protecting Privacy from Aerial Surveillance*. Washington, DC: American Civil Liberties Union, 2011.

Darnell, Bart W. "Unmanned Aircraft Systems: A Logical Choice for Homeland Security Support." Master's thesis, Naval Postgraduate School, 2011.

Department of Defense. *Unmanned Systems Roadmap 2007–2032*.Washington, DC: Department of Defense, 2007.

Diaz, Monica. "Arlington Police Hopeful Their Drones Will Soon be Taking Flight." *WFAA News*, February 7, 2013. http://www.wfaa.com/news/local/tarrant/Arlington-police-hopeful-their-drones-will-soon-be-taking-flight-190325001.html.

European Commission. “Why Do We Need an EU Data Protection Reform.” Accessed August 20, 2013. http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

Eyerman, Joe, Ken Hinkle, Clark Letterman, David Schanzer, Wayne Pitts, Katrina Ladd, John Holloway, Susan Mitchell, Wayne Pitts and S. Cornelia Kaydos-Daniels. *Unmanned Aircraft and the Human Element: Public Perceptions and First Responder Concerns*. Research Triangle Park, NC: Institute for Homeland Security Solutions, 2013.

Francescani, Chris. “From Hollywood to Kansas, Drones Are Flying under the Radar.” *Reuters*. March 3, 2013. http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303.

———. “Unmanned Aircraft Systems (UAS) Infographic.” Accessed January 2, 2014. http://www.faa.gov/about/initiatives/uas/infographic/

Dillingham Gerald L. *Unmanned Aircraft Systems, Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*. GAO-12-981. Washington, DC: Government Accountability Office, 2012.

GOV.UK. “The Data Protection Act.” Accessed August 20, 2013. https://www.gov.uk/data-protection/the-data-protection-act.

Gertler, Jeremiah. *U.S. Unmanned Aerial Systems*. CRS Report R42136. Washington, DC: Library of Congress, Congressional Research Service, January 23, 2012.

Harrison, Glennon J. *Unmanned Aircraft Systems Manufacturing Trends*. CRS Report R42938, Washington, DC: Library of Congress, Congressional Research Service, 2013.

Human Rights Watch. *Losing Humanity: The Case against Killer Robots*. New York: Human Rights Program Watch, November 19, 2012.

International Association of Chiefs of Police Aviation Committee. “Recommended Guidelines for the Use of Unmanned Aircraft.” Accessed August 16, 2013. http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

Journeyman TV. *Rise of the Machines*, online documentary, ABC Australia, produced by Mark Corcoran and Janet E. Silver, October 15, 2012. http://www.journeyman.tv/?lid=64311.

Kahneman, Daniel. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kirkpatrick, Marshall. "Facebook's Zuckerberg Says the Age of Privacy Is Over." *Readwrite*, January 9, 2010. http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~ofrKLp0EphACyi.

Levin, Alan, and Jeff Plungis, "Pilots Say Go Slow on Commercial Drones after Ditching." *Bloomberg*. January, 29, 2014. http://www.bloomberg.com/news/2014-01-28/customs-drone-fleet-grounded-after-predator-goes-down.html.

Marsa, Linda. "A Wing and a Prayer: The U.S.'s Crumbling Air-Travel Infrastructure." *Discover Magazine*, October 22, 2009. http://discovermagazine.com/2009/sep/22-wing-and-prayer-us-crumbling-air-travel-infrastructure#.UVi8QheG3hc.

Melito, Thomas. *Nonproliferation: Agencies Could Improve Information Sharing and End Use Monitoring on Unmanned Aerial Vehicle Exports*. GAO -12-536, Washington, DC: Government Accountability Office, 2012.

Moghaddam, Fathali M. *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*. Westport, CT: Praeger, 2006.

Monmouth University Poll. *National: U.S. Supports Unarmed Domestic Drones But Public Prefers Requiring Court Orders First*. West Long Branch, NJ: Monmouth University, August 13, 2013. https://www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/409aecfb-3897-4360-8a05-03838ba69e46.pdf.

Moore's Law. "Moore's Law or How Overall Processing Power will Double Every Two Years." Accessed March 2, 2014. http://www.mooreslaw.org/.

Moose, Robert G. "Covering The Homeland: National Guard Unmanned Aircraft Systems Support for Wildland Firefighting And Natural Disaster Events." Master's thesis, Naval Postgraduate School, 2008.

Mozdzanowski, Aleksandra, Roland E. Weibel, and R. John Hansman. "Feedback Model of Air Transportation System Change: Implementation Challenges for Aviation Information Systems." *Proceedings of the IEEE* 96, no. 12 (2008): 1977–1978. https://ieeexplore.ieee.org/ieee_pilot/articles/96jproc12/jproc-RWeibel-2006118/article.html.

NASA. "Unmanned Aircraft Systems Airspace Operations Challenge (UAS AOC)." Accessed January 6, 2014. http://www.nasa.gov/directorates/spacetech/centennial_challenges/uas/index.html#.UuWVStLTnDc.

Nieto-Gomez, Rodrigo. "Power of 'the Few': The Key Strategic Challenge for the Permanently Disrupted High-Tech Homeland Security Environment" *Homeland Security Affairs* 7, 2011. https://www.hsaj.org/?fullarticle=7.1.18.

Privacy International, “Map of Surveillance Societies around the World, accessed August 20, 2013. https://www.privacyinternational.org /sites/privacyinternational.org/files/file-downloads/phrcomp_sort_0.pdf.

Rafter, Isolde. “Anticipating Domestic Boom, Colleges Rev up Drone Piloting Programs.” *NBCNews.com*, January 29, 2013.

Scott W. Walker. “Integrating Department of Defense Unmanned Aerial Systems into the National Airspace Structure.” Master’s thesis, U.S. Army Command and General Staff College, 2010.

Segal, Adam. “Chinese Computer Games: Keeping Safe in Cyberspace.” *Foreign Affairs* 91, no. 2 (March/April 2012):16

Sengupta, Somini. “Rise of Drones in U.S. Drives Efforts to Limit Police Use.” *New York Times*, February 15, 2013.

Singer, Peter W. “The Predator Comes Home: A Primer on Domestic Drones, their Huge Business Opportunities, and their Deep Political, Moral and Legal Challenges.” *Brookings Institute*, March 8, 2013. http://www.brookings.edu/research/papers/2013/03.08-drones-singer (accessed April 2013).

———. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Books. 2009.

Suarez, Daniel. “The Kill Decision Shouldn’t Belong to a Robot.” *Ted Talks*, posted June 2013. http://www.ted.com/talks/daniel_suarez_the_kill _decision_shouldn_t_belong_to_a_robot.html.

Tadjdeh, Yasmin. “New Senate Unmanned Aerial Vehicle Caucus to Tackle Privacy Issues.” *National Defense Magazine.* December 2012. http://www.nationaldefensemagazine.org/archive/2012/December/Pages/NewSenateUnmannedAerialVehicleCaucustoTacklePrivacyIssues.aspx.

Teal Group. “Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast.” News release, April 11, 2012. http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/66-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast.

Thompson, Richard M. *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Respo*nses. CRS Report R42701. Washington, DC: Library of Congress, Congressional Research Service, April 3, 2013.

U.S. Air Force. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009–2047* Washington, DC: USAF Headquarters, May 18, 2009.

U.S. Army. *U.S. Army Unmanned Aircraft Systems Roadmap* 2010–2035. Fort Rucker, AL: U.S. Army Center of Excellence, 2010.

U.S. Navy. "X-47B Operates Aboard Theodore Roosevelt." News release, November 10, 2013. http://www.navy.mil/submit/display.asp?story_id=77580.

Unmanned Systems Caucus. "Congressional Unmanned Systems Caucus." Accessed January 14, 2014. http://unmannedsystemscaucus.mckeon.house.gov /about/purpose-mission-goals.shtml.

Yadav, Yatich. "UAVs Prone to Hacking, Warn Intel Agencies." *Indian Express*, July 25, 2013. http://www.newindianexpress.com/nation/UAVs-prone-to-hacking-warn-intel-agencies/2013/07/25/article1700651.ece#.UwkD0mJdXhc.

Zimbardo, Philip. *The Lucifer Effect: Understanding how Good People Turn Evil*. New York: Random House, 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California